bitdefender
BUSINESS SOLUTIONS

SECURITY FOR SAMBA

User's guide

bitdefender

BitDefender Security for Samba

User's guide

Published 2009.10.29
Revision Version 1.2.2478

Copyright© 2009 BitDefender

Table of Contents

End User Software License Agreement viii

Preface xii

1. Conventions used in this book xii
   1.1. Typographical conventions xii
   1.2. Admonitions xiii
2. Book structure xiv
3. Request for Comments xv

Description 1

1. Features and Benefits 2

1.1. Key Features 2
1.2. Key Benefits 2

2. BitDefender architecture 4

2.1. The core modules 4
2.2. Samba integration 6

Installation 7

3. Prerequisites 8

3.1. System Requirements 8
   3.1.1. Hardware system requirements 8
   3.1.2. Software system requirements 8
   3.1.3. File server requirements 9
3.2. Package naming convention 9
   3.2.1. Linux convention 9
   3.2.2. FreeBSD convention 10

4. Package installation 11

4.1. Getting BitDefender Security for Samba 11
   4.1.1. BitDefender Software Repositories 11
4.2. Install the package 12
   4.2.1. Install the Linux packages 12
   4.2.2. Install the FreeBSD packages 14
   4.2.3. Install the language package 16
4.3. The installer 17

5. Uninstall 18

5.1. Uninstall the rpm package 18
5.2. Uninstall the deb package 18
5.3. Uninstall the ipk package 18

5.4. Uninstall the tbz package 19

Getting Started 20

6. Start-up and Shut-down 21
6.1. Start-up 21
6.2. Shut-down 22
6.3. Restart 23

7. BitDefender Status Output 24
7.1. Process Status 24
7.2. Basic Information 24
7.3. Statistical Report 25

8. Fileserver Integration 26
8.1. Compiling Samba 26

Advanced Usage 28

9. Configuration 29
9.1. Basic Configuration 29
9.1.1. Samba VFS Module Configuration 30
9.2. The BitDefender Logger Daemon 31
9.2.1. The Logger Plugins 32
9.3. Quarantine 33

10. Product Registration 36

11. Testing BitDefender 37
11.1. Antivirus Test 37

12. Updates 38
12.1. Automatic Update 38
12.1.1. Time Interval Modification 38
12.1.2. Live! Update Proxy Configuration 39
12.2. Manual Update 40
12.3. Patches and New Product Versions 40

Remote Management 42

13. BitDefender Remote Admin 43
13.1. Getting Started 43
13.2. Status 44
13.2.1. Services 44
13.2.2. License 45
13.2.3. About 47
13.3. Quarantine 48

13.3.1. Samba Quarantine 48
13.3.2. Deferred Quarantine 50
13.4. Components 51
13.4.1. Samba 51
13.5. Maintenance 54
13.5.1. Live! Update 54
13.5.2. Patches 55
13.5.3. Users 55
13.5.4. Global Proxy 56
13.6. Reports 57
13.6.1. Statistics 57
13.6.2. Charts 58
13.7. Logging 59
13.7.1. File Logging 60
13.7.2. Mail Alerts 61

14. SNMP 62
14.1. Introduction 62
14.2. The SNMP Daemon 62
14.3. The BitDefender Logger Plugin 63
14.3.1. Prerequisites 63
14.3.2. Configuration 64
14.3.3. Usage 66
14.4. Troubleshooting 67

15. BitDefender Client Security 68
15.1. Introduction 68

Getting Help 69

16. Support 70
16.1. Support department 70
16.2. On-line help 70
16.2.1. BitDefender Knowledge Base 70
16.2.2. BitDefender Unix Servers Mailing List 71
16.3. Online Forum 72
16.4. Contact information 72
16.4.1. Web Addresses 72
16.4.2. BitDefender Offices 72

Appendices 75

A. Supported antivirus archives and packs 76

B. Alert templates 78
B.1. Variables 78

B.2. Sample results 79
B.2.1. FileServer Alert 79
B.2.2. KeyWillExpire Alert 80
B.2.3. KeyHasExpired Alert 81
Glossary 82

End User Software License Agreement

IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS DO NOT INSTALL THE SOFTWARE. BY SELECTING "I ACCEPT", "OK", "CONTINUE", "YES" OR BY INSTALLING OR USING THE SOFTWARE IN ANY WAY, YOU ARE INDICATING YOUR COMPLETE UNDERSTANDING AND ACCEPTANCE OF THE TERMS OF THIS AGREEMENT.

These Terms cover BitDefender Corporate Solutions and Services for Companies licensed to you, including related documentation and any update and upgrade of the applications delivered to you under the purchased license or any related service agreement as defined in the documentation and any copy of these items.

This License Agreement is a legal agreement between you (either an individual or a legal person) and BITDEFENDER for use of BITDEFENDER's software product identified above, which includes computer software and services, and may include associated media, printed materials, and "online" or electronic documentation (hereafter designated as "BitDefender"), all of which are protected by international copyright laws and international treaties. By installing, copying or using BitDefender, you agree to be bound by the terms of this agreement. If you do not agree to the terms of this agreement, do not install or use BitDefender.

BitDefender License. BitDefender is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. BitDefender is licensed, not sold.

GRANT OF LICENSE. BITDEFENDER hereby grants you and only you the following non-exclusive, limited, non-transferable and royalty-bearing license to use BitDefender.

APPLICATION SOFTWARE. You may install and use BitDefender, on as many computers as necessary with the limitation imposed by the total number of licensed users. You may make one additional copy for back-up purpose.

SERVER USER LICENSE. This license applies to BitDefender software that provides network services and can be installed on computers that provide network services. You may install this software on as many computers as necessary within the limitation imposed by the total number of users to which these computers provide network services. This limitation refers to the total number of users that has to be less than or equal to the number of users of the license.

DESKTOP USER LICENSE. This license applies to BitDefender software that can be installed on a single computer and which does not provide network services. Each primary user may install this software on a single computer and may make one

additional copy for backup on a different device. The number of primary users allowed is the number of the users of the license

TERM OF LICENSE. The license granted hereunder shall commence on the purchasing date of BitDefender and shall expire at the end of the period for which the license is purchased.

EXPIRATION. The product will cease to perform its functions immediately upon expiration of the license.

UPGRADES. If BitDefender is labeled as an upgrade, you must be properly licensed to use a product identified by BITDEFENDER as being eligible for the upgrade in order to use BitDefender. A BitDefender labeled as an upgrade replaces and/or supplements the product that formed the basis for your eligibility for the upgrade. You may use the resulting upgraded product only in accordance with the terms of this License Agreement. If BitDefender is an upgrade of a component of a package of software programs that you licensed as a single product, BitDefender may be used and transferred only as part of that single product package and may not be separated for use by more than the total number of licensed users. The terms and conditions of this license replace and supersede any previous agreements that may have existed between you and BITDEFENDER regarding the original product or the resulting upgraded product.

COPYRIGHT. All rights, titles and interest in and to BitDefender and all copyright rights in and to BitDefender (including but not limited to any images, photographs, logos, animations, video, audio, music, text, and "applets" incorporated into BitDefender), the accompanying printed materials, and any copies of BitDefender are owned by BITDEFENDER. BitDefender is protected by copyright laws and international treaty provisions. Therefore, you must treat BitDefender like any other copyrighted material. You may not copy the printed materials accompanying BitDefender. You must produce and include all copyright notices in their original form for all copies created irrespective of the media or form in which BitDefender exists. You may not sub-license, rent, sell, lease or share the BitDefender license. You may not reverse engineer, recompile, disassemble, create derivative works, modify, translate, or make any attempt to discover the source code for BitDefender.

LIMITED WARRANTY. BITDEFENDER warrants that the media on which BitDefender is distributed is free from defects for a period of thirty days from the date of delivery of BitDefender to you. Your sole remedy for a breach of this warranty will be that BITDEFENDER, at its option, may replace the defective media upon receipt of the damaged media, or refund the money you paid for BitDefender. BITDEFENDER does not warrant that BitDefender will be uninterrupted or error free or that the errors will

be corrected. BITDEFENDER does not warrant that BitDefender will meet your requirements.

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, BITDEFENDER DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THE PRODUCTS, ENHANCEMENTS, MAINTENANCE OR SUPPORT RELATED THERETO, OR ANY OTHER MATERIALS (TANGIBLE OR INTANGIBLE) OR SERVICES SUPPLIED BY HIM. BITDEFENDER HEREBY EXPRESSLY DISCLAIMS ANY IMPLIED WARRANTIES AND CONDITIONS, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INTERFERENCE, ACCURACY OF DATA, ACCURACY OF INFORMATIONAL CONTENT, SYSTEM INTEGRATION, AND NON-INFRINGEMENT OF THIRD PARTY RIGHTS by filtering, disabling, or removing such third party's software, spyware, adware, cookies, emails, DOCUMENTS, advertisements or the like, WHETHER ARISING BY STATUTE, LAW, COURSE OF DEALING, CUSTOM AND PRACTICE, OR TRADE USAGE.

DISCLAIMER OF DAMAGES. Anyone using, testing, or evaluating BitDefender bears all risk to the quality and performance of BitDefender. In no event shall BITDEFENDER be liable for any damages of any kind, including, without limitation, direct or indirect damages arising out of the use, performance, or delivery of BitDefender, even if BITDEFENDER has been advised of the existence or possibility of such damages.

SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

IN NO CASE SHALL BITDEFENDER'S LIABILITY EXCEED THE PURCHASE PRICE PAID BY YOU FOR BITDEFENDER. The disclaimers and limitations set forth above will apply regardless of whether you accept to use, evaluate, or test BitDefender.

IMPORTANT NOTICE TO USERS. THIS SOFTWARE IS NOT FAULT-TOLERANT AND IS NOT DESIGNED OR INTENDED FOR USE IN ANY HAZARDOUS ENVIRONMENT REQUIRING FAIL-SAFE PERFORMANCE OR OPERATION. THIS SOFTWARE IS NOT FOR USE IN THE OPERATION OF AIRCRAFT NAVIGATION, NUCLEAR FACILITIES, OR COMMUNICATION SYSTEMS, WEAPONS SYSTEMS, DIRECT OR INDIRECT LIFE-SUPPORT SYSTEMS, AIR TRAFFIC CONTROL, OR ANY APPLICATION OR INSTALLATION WHERE FAILURE COULD RESULT IN DEATH, SEVERE PHYSICAL INJURY OR PROPERTY DAMAGE.

GENERAL. This Agreement will be governed by the laws of Romania and by international copyright regulations and treaties. The exclusive jurisdiction and venue to adjudicate any dispute arising out of these License Terms shall be of the courts of Romania.

Prices, costs and fees for use of BitDefender are subject to change without prior notice to you.

In the event of invalidity of any provision of this Agreement, the invalidity shall not affect the validity of the remaining portions of this Agreement.

BitDefender and BitDefender logos are trademarks of BITDEFENDER. All other trademarks used in the product or in associated materials are the property of their respective owners.

The license will terminate immediately without notice if you are in breach of any of its terms and conditions. You shall not be entitled to a refund from BITDEFENDER or any resellers of BitDefender as a result of termination. The terms and conditions concerning confidentiality and restrictions on use shall remain in force even after any termination.

BITDEFENDER may revise these Terms at any time and the revised terms shall automatically apply to the corresponding versions of the Software distributed with the revised terms. If any part of these Terms is found void and unenforceable, it will not affect the validity of rest of the Terms, which shall remain valid and enforceable.

In case of controversy or inconsistency between translations of these Terms to other languages, the English version issued by BITDEFENDER shall prevail.

Contact BITDEFENDER, at Preciziei Boulevard, no. 24, West Gate Building H2, ground floor, 6th district, Bucharest, Romania, or at Tel No: 40-21-2330780 or Fax:40-21-2330763, e-mail address: office@bitdefender.com

Preface

This *User's guide* is intended for all System Administrators who have chosen BitDefender Security for Samba as security solution for their File Servers. The information presented in this book is suitable not only for computer literates, it is accessible to everyone who is able to do administrative tasks on a Linux or UNIX box.

This book will describe for you BitDefender Security for Samba, the Company and the team who built it, it will guide you through the installation process, teach you how to configure it to the very detail. You will find out how to use BitDefender Security for Samba, how to update, interrogate, test and customize it. You will learn how to integrate it with various software and how to get the best from BitDefender.

We wish you a pleasant and useful reading.

1. Conventions used in this book

1.1. Typographical conventions

Several text styles are used in the book for an improved readability. Their aspect and meaning are presented in the table below.

Appearance	*Description*
`variable`	Variables and some numerical data are printed with `monospaced` characters.
http://www.bitdefender.com	The URL links point to some external location, on http or ftp servers.
support@bitdefender.com	Emails are inserted in the text for contact information.
Chapter 4 "*Package installation*" (p. 11)	This is an internal link, towards some location inside the document.
`filename`	File and directories are printed using `monospaced` font.
`ENV_VAR`	Environment variables are `MONOSPACED CAPITALS`.

Appearance	*Description*
emphasized	*Emphasized text* specially marked to call your attention.
“quoted text”	Provided as reference.
command	Inline commands are printed using **strong** characters.
`# command -parameter`	Command examples are printed in strong monospaced characters in a specially marked environment. The prompt can be one of the following. **#** The root prompt. You should be root in order to run this command. **$** The normal user prompt. You do not need special privileges to run the command.
`screen output`	Screen output and code listings are printed in monospaced characters in a specially marked environment.
bdlogd(8)	It refers to a man page.

1.2. Admonitions

Admonitions are in-text notes, graphically marked, offering additional information related to the current paragraph.

Note
The note is just a short observation. Although you can omit them, notes can provide valuable information, such as a specific feature or a link to some related topic.

Important
This requires your attention and it is not recommended to skip it. Usually, it provides non-critical but significant information.

Warning
This is critical information you should treat with increased caution. Nothing bad will happen if you follow the indications. You should read and understand it, because it describes something extremely risky.

2. Book structure

The book consists of four parts, containing the following major topics: Description and features, Installation, Usage and Getting help. Moreover, a glossary and UNIX manual pages are provided to clarify different aspects of BitDefender, which could cause technical problems.

Description. A short introduction to BitDefender. It explains who is BitDefender, and the Data Security Division. You are presented BitDefender Security for Samba, its features, the product components and the basics of the integration and the scanning mechanism.

Installation. Step by step instructions for installing BitDefender on a system. Starting with the prerequisites for a successful installation, you are guided through the whole installation process. Finally, the uninstall procedure is described in case you need to uninstall BitDefender.

Getting Started. Description of basic administration and maintenance of BitDefender.

Advanced Usage. You are presented the BitDefender configuration tools, how to get run-time information, how to test antivirus efficiency, how to perform updates and how to register the product.

Remote Management. You will learn how to make the best of BitDefender remotely, by using several remote administration tools.

Getting Help. Where to look and where to ask for help if something goes not so right. You are presented the Knowledge Base and offered the BitDefender and BitDefender partners contact information to call, if needed.

Appendices. The Appendices present exhaustive information about configuration, email templates and in-depth discussions over tricky parts.

Glossary. The Glossary tries to explain some technical and uncommon terms you will find in the pages of this book.

3. Request for Comments

We invite you to help us improve the book. We have tested and verified all of the information to the best of our ability, but you may find that features have changed (or even that we have made mistakes). Please write to tell us about any flaws you find in this book or how you think it could be improved, to help us provide you the best documentation possible.

Let us know by sending an email to documentation@bitdefender.com.

Description

1. Features and Benefits

Efficient Antimalware Protection for Samba Network Shares. BitDefender Security for Samba provides antivirus and antispyware protection for Samba network shares. By scanning all accessed files for known and unknown malware it keeps network users safe and it helps comply with data protection regulations. Highly flexible, the open source BitDefender vfs module can be compiled against any Samba version, rendering it the ideal choice for your favorite Unix-based system.

1.1. Key Features

- Proactive heuristic protection against zero-day threats
- Supports different actions or settings for each protected share
- SNMP monitoring systems support
- Flexible and intuitive remote management interface
- Complies with all major Linux distributions
- Available in both 32-bit and 64-bit versions

1.2. Key Benefits

Compatibility

- Features a pre-compiled version of the vfs module, allowing integration with the latest Samba build available
- Works with any Samba build and can be easily compiled against all versions, thanks to its open-sourced vfs module
- Fully complies with FHS (Filesystem Hierarchy Standard), operating in a completely non-intrusive manner
- Ensures compatibility with all major Unix-based platforms due to its rpm, deb and generic .tar.run packages

Safe Sharing of Files and Documents

- Enables safe file and document sharing by adapting its actions to the malware type detected

- Provides the possibility of separately handling riskware (applications that pose a potential threat, but which certain user groups might still need)
- Uses a built-in "Pipe to program" action, which allows you to feed the objects detected by the BitDefender engines to scripts or to other programs
- Allows you to define more than one quarantine area, searchable based on regular expressions, sender, recipient, date and cause for quarantine

Increased Usability

- Allows you to define separate sets of antivirus rules for each protected share resulting in better compliance with specific file sharing policies
- Allows performing management actions via SNMP by means of its SNMP Daemon Plug-in
- Can send customizable e-mail notifications or SNMP alerts about its activity: number of scanned, disinfected, deleted, infected or filtered files
- Comes with an intuitive management interface, BitDefender Remote Admin, which helps remotely configure any settings and check the current or past activity of the solution (detailed statistics, graphs and charts)
- Offers an alternative command line interface, BDSAFE (The BitDefender Swiss Army KniFE), which allows performing post-install configuration and administration tasks

Centralized Management Support

BitDefender Management Server allows centralized management for most BitDefender business solutions installed on network computers, including BitDefender Security for Samba. This type of integration allows you to use the Management Server console to get centralized access to:

- configuration settings for BitDefender Security for Samba
- critical event information such as update-related events, configuration warnings, license expiration
- easy-to-interpret statistics and reports based on the information received from BitDefender Security for Samba

2. BitDefender architecture

BitDefender is a highly complex modular structure. It is made up of several central components and additional modules, each of them having assigned a specific task. The modules are loaded during BitDefender startup and enabled or not, according to the user's preferences. On a UNIX-like system, these components run as daemons, on one or multiple threads, and communicate with the others.

2.1. The core modules

Listed by their file names, the core modules are represented in the following table.

Module	*Description*
bdmond	The BitDefender Core Monitor is the supervisor of several BitDefender modules. When one of them crashes, the Core Monitor isolates the object causing the crash in a special quarantine directory, notifies the administrator and restarts the involved module. Thus, even if one process dies, the whole filtering activity is not disturbed, ensuring continuous server protection.
bdscand	This is the BitDefender Scan Daemon. Its purpose is to integrate the scanning engines, receive scanning requests from several daemons, such as the mail daemon or the file daemon. It scans the objects, takes the necessary actions and sends back the object and the scanning results.
bdfiled	The BitDefender File Daemon has the role of receiving scanning requests from the Samba Virtual Filesystem module. It calls the Scan Daemon to perform the scan, expecting the scanning results from it. Then it applies his actions and sends back the results to Samba.
bdregd	The BitDefender Registry is made up of the **bdregd** program and a set of XML files, where it stores the BitDefender configuration. The daemon receives requests to read from and to write to the settings file, requests initiated by the other processes. The Registry can receive requests from other hosts too, using a secured tcp connection on port `8138`. All remote communication is done using SSL (Secure Socket Layer). This is only useful when you are using some Remote Admin Console, eventually running on some non-UNIX Operating System. If

Module	Description
	not, for security reasons, it is recommended to keep this feature disabled (it is disabled by default). ***Manually editing the Registry*** Even if the XML files are human-readable (and writable, too), you should never try to edit them manually. Due to their high complexity, the XML files should only be modified by means of the provided configuration tools, such as the **bdsafe** command or the Remote Administration Consoles.
bdlogd	The BitDefender Logger is a complex component, handling all logging and notification actions of BitDefender. There are several types of logging, all of them realized by plugins. ● *file logging:* the data is sent to a normal log file, respecting a typical format. ● *mail notification:* alerts are sent by email to the server administrator or to the sender and the recipients of an email, on special events (such as infected email found). ● *Real Time Virus and Spam Report:* anonymous statistics are sent to BitDefender Labs to keep a map of malware activity and to detect outbreaks. ● *SNMP:* notifications can be sent through the SNMP protocol to designated hosts.
bdlived	The BitDefender Live! Update is the module responsible with updating the scanning engines and some other BitDefender components. The module runs continuously and periodically checks the update server. It can also be triggered manually or by the Update Pushing mechanism. ***More about Live! Update*** BitDefender Live! Update and the update process are described in Chapter 12 "*Updates*" (p. 38).
bdsnmpd	**bdsnmpd** accepts SNMP GET and SET messages related to BitDefender registry keys. Thus, an authorized user is able to read and modify some of the BitDefender configuration settings remotely.

2.2. Samba integration

The Samba fileserver supports global and per-share Virtual FileSystem Plugins. The BitDefender VFS module acts as Samba integration agent: aware of the files requested by clients, it can call the BitDefender core to scan the requested files. It receives the scanning results and applies the configured actions, if the file is infected. Furthermore, Samba will act accordingly, allowing or denying client access.

Installation

3. Prerequisites

BitDefender Security for Samba can be installed on package-based Linux distributions (rpm or deb) and tbz based FreeBSD versions. Other distributions are supported by using the ipkg package system, with the same functionality. The packages include all the necessary pre-install, post-install, pre-remove and post-remove scripts. The adequate package type should be installed according to the distribution.

3.1. System Requirements

Before installing BitDefender Security for Samba, you must verify that your system meets the following system requirements:

3.1.1. Hardware system requirements

Processor type

x86 compatible, minimum 800MHz, but do not expect great performance in this case. An i686 generation processor, running at 1.4Ghz, would make a better choice.

Memory

The minimum accepted value is 128MB (recommended is at least 256MB, for a better performance).

Free disk space

The minimum free disk space to install and run BitDefender Security for Samba is 60MB. But the log and the quarantine directories will require more space - 200MB of free space would be welcome.

Internet connection

Although BitDefender Security for Samba will run with no Internet connection, the update procedure will require an active HTTP link, even through some proxy server. Therefore, for an up to date protection, the Internet connection is a MUST.

3.1.2. Software system requirements

Linux requirements

The Linux kernel should be at least 2.6.18.

BitDefender requires `glibc` version 2.3.1, or newer, and `libstdc++` from `gcc 4` or newer.

The supported Linux distributions are the next ones:

- RedHat enterprise Linux 3 or newer
- SuSE Linux Enterprise Server 9 or newer
- Suse Linux 8.2 or newer
- RedHat Linux 9
- Fedora Core 1 or newer
- Debian GNU/Linux 3.1 or newer
- Slackware 9.x or newer
- Mandrake/Mandriva 9.1 or newer
- Gentoo 1.4 or newer

FreeBSD requirements:

The supported FreeBSD versions are 5.4-RELEASE or newer.

The FreeBSD older versions are no longer supported.

3.1.3. File server requirements

At the release date, BitDefender Security for Samba fully supports Samba version 3.x. Further versions will be supported as they appear. If you have another version and there is no precompiled BitDefender VFS module, you have to get the sources from `/opt/BitDefender/var/src` directory and compile them yourself. For more about this, please see the install notes accompanying the BitDefender VFS module.

If you do not have Samba installed, you must download the source code, compile and install it.

3.2. Package naming convention

The BitDefender Security for Samba package is named considering the following scheme:

3.2.1. Linux convention

Linux packages are named according to the following rule.

```
BitDefender-Security-Samba-{ver}-{os}-{arch}.{pkg}.run
```

Variable	Description
{ver}	This is the package version. For example, 2.1-1 is version 2, subversion 1, package build 1.
{os}	The operating system is Linux, with GCC 4.x compiler.
{arch}	The architecture contains the processor class. i586 and amd64 are the current versions.
{pkg}	This stands for the package management tool name. Therefore, it is rpm for Red Hat Manager, deb for Debian and ipk for IPKG.

3.2.2. FreeBSD convention

There are two FreeBSD packages, namely:

```
bitdefender-common-{ver}.tbz
  bitdefender-samba-{ver}.tbz
```

Where *{ver}* is the package version. For example, 2.1_1 is version 2, subversion 1, package build 1.

4. Package installation

This chapter explains how to install BitDefender on a Unix-like system, such as Linux or FreeBSD. This is pretty straightforward: get the desired package, test it for integrity, then install it.

4.1. Getting BitDefender Security for Samba

The package can be downloaded from the BitDefender servers or it can be found on different distribution media, such as CD-ROM. When downloading from the BitDefender servers, you will be asked to fill in a form and you will receive an email on the address you have provided in this form. The email contains the download location.

The Linux packages come in three flavours:

- `rpm` for distributions using the RedHat Linux package management
- `deb` for distributions using Debian Linux packaging system
- `ipk` for any other distribution using IPKG, the Itsy Package Management System

The FreeBSD packages are `tbz` (.tar.bz) compressed archives, adequate for FreeBSD starting from version 5.

4.1.1. BitDefender Software Repositories

In order to make our products more accessible, BitDefender offers its own `deb` and `rpm` software repositories.

To add the BitDefender repository to a Debian based distribution, follow these steps:

1. Add the BitDefender repository key to the list of **apt** trusted keys by running the following commands:

```
$ wget http://download.bitdefender.com/repos/deb/bd.key.asc
```

```
# apt-key add bd.key.asc
```

2. Add the following line to the `/etc/apt/sources.list` file:

```
deb http://download.bitdefender.com/repos/deb/ bitdefender  \
      non-free
```

3. Refresh your **apt** cache by running one of the following commands:

```
$ apt-get update
```

or

```
$ aptitude update
```

To add the BitDefender repository to a RedHat based distribution, follow these steps:

1. Install the BitDefender-repo package:

```
$ rpm -i http://download.bitdefender.com/repos/rpm/    \
      bitdefender/i586/BitDefender-repo-1-1.noarch.rpm
```

2. Update the **yum** cache:

```
$ yum update
```

4.2. Install the package

There is a common installation method for `rpm`, `deb` and `ipk`, as well as several methods for FreeBSD.

4.2.1. Install the Linux packages

The packages should be installed using the following command:

```
# sh BitDefender-Security-Samba-{ver}-{os}-{arch}.{pkg}.run
```

This will unpack the BitDefender packages, according to the package type, and install them using the package manager. The packages contain the BitDefender files (engines, core, etc.), the install and uninstall scripts.

Let's take some examples.

To install BitDefender Security for Samba on a RedHat based distribution you have to run the following command:

```
# sh BitDefender-Security-Samba-{ver}-{os}-{arch}.rpm.run
```

If you have set up your system to use the BitDefender software repository, you can install BitDefender Security for Samba using your prefered **yum** front-end. For example:

```
# yum install BitDefender-Samba
```

To install BitDefender Security for Samba on a Debian based distribution you have to run the following command:

```
# sh BitDefender-Security-Samba-{ver}-{os}-{arch}.deb.run
```

If you have set up your system to use the BitDefender software repository, you can install BitDefender Security for Samba using your prefered **apt** front-end. For example:

```
# apt-get install bitdefender-samba
```

The `ipk` version of the archive will install the **ipkg** tools on the system and will use them to install the `.ipk` packages.

To install BitDefender Security for Samba on any Linux distribution, using **ipkg**, you have to run the following command:

```
# sh BitDefender-Security-Samba-{ver}-{os}-{arch}.ipk.run
```

Additional parameters

For the not-so-impatient user, the self-extractable archive provides some command line parameters, described in the following table:

Parameter	Description
`--help`	Prints the short help messages.
`--info`	This will print the archive information, such as the title, the default target directory, the embedded script to be run after unpacking, the compression method used, the uncompressed size, the packaging date.
`--list`	This option will print the content of the embedded archive. The listed files are the engines, the program binaries, the embedded documentation, the install and uninstall script along with their size and permissions.

`--check`	This is one of the most useful options, because it enables the user to verify package integrity, as stated above. The integrity is checked comparing the embedded md5 checksum (generated during packaging) with the one computed at the time of the check. If they match, the output will be the following:
	`MD5 checksums are OK. All good.`
	If not, an error message will be shown, displaying the non-matching stored and computed checksums, as follows:
	`Error in MD5 checksums: X is different from Y`

`--confirm`	The user will be asked to confirm every step of the install process.
`--keep`	By default, the archive content is extracted to a temporary directory, which will be removed after the embedded installer exits. Adding this parameter to the script will not remove the directory.
`--target` *directory*	You can specify another directory to extract the archive to, if you don't want to use the default name. Note that this target directory will not be removed.
`--uninstall`	Run the embedded uninstaller script instead of the normal installer.

4.2.2. Install the FreeBSD packages

The packages should be installed using the following command:

```
# sh BitDefender-Security-Samba-{ver}-{os}-{arch}.tbz.run
```

This will unpack the BitDefender packages, according to the package type, and install them using the package manager. The packages contain the BitDefender files (engines, core, etc.), the install and uninstall scripts.

Additional parameters

For the not-so-impatient user, the self-extractable archive provides some command line parameters, described in the following table:

Parameter	Description
`--help`	Prints the short help messages.
`--info`	This will print the archive information, such as the title, the default target directory, the embedded script to be run after unpacking, the compression method used, the uncompressed size, the packaging date.
`--list`	This option will print the content of the embedded archive. The listed files are the engines, the program binaries, the embedded documentation, the install and uninstall script along with their size and permissions.

`--check`	This is one of the most useful options, because it enables the user to verify package integrity, as stated above. The integrity is checked comparing the embedded md5 checksum (generated during packaging) with the one computed at the time of the check. If they match, the output will be the following:
	`MD5 checksums are OK. All good.`
	If not, an error message will be shown, displaying the non-matching stored and computed checksums, as follows:
	`Error in MD5 checksums: X is different from Y`

`--confirm`	The user will be asked to confirm every step of the install process.

Parameter	Description
`--keep`	By default, the archive content is extracted to a temporary directory, which will be removed after the embedded installer exits. Adding this parameter to the script will not remove the directory.
`--target` *directory*	You can specify another directory to extract the archive to, if you don't want to use the default name. Note that this target directory will not be removed.
`--uninstall`	Run the embedded uninstaller script instead of the normal installer.

4.2.3. Install the language package

You have the possibility to choose the language you are familiar with at install time. By doing so, the help messages, error messages, etc. will be displayed in accordance with your choice.

To install the language package on your computer, you just have to run the following command:

```
# sh BitDefender-Security-Samba-langpack-{ver}-{os}-\
    {arch}.{pkg}.run
```

It automatically detects the language of the system locale via the LANG environment variable.

The language localization files will be placed under the following directory: `/opt/BitDefender/share/locale/[lang]/`.

A link pointing to `/opt/BitDefender/share` will be made as `/usr/share/bitdefender`.

However, if you are dissatisfied with the chosen language, you can configure this option, setting another language to display in. This can be done either by changing the value of the LANG variable or by using a configuration key together with **bdsafe** tool.

This is the command you should run if you have decided to use **bdsafe** tool.

```
# bdsafe lang LL_CC.UTF-8
```

LL stands for language code (ISO 639) and CC for country code (ISO 3166). For example, if you want to set the language to display in to be Romanian, run the command:

```
# bdsafe lang ro_RO.UTF-8
```

Important
Your terminal must support **UTF-8** encoding.

If you didn't install the language pack in the first place, just install it through the package manager any time you like.

4.3. The installer

After unpacking the archive, the installer is launched. This is a text based installer, created to run on very different configurations. Its purpose is to install the extracted packages to their locations and to make the first configuration of BitDefender Security for Samba, while asking you few questions. To accept the default configuration the installer offers (which is recommended), just press the ENTER key when prompted.

First, the *License Agreement* is displayed. You are invited to read the full content by pressing the SPACE bar to go to the next page or ENTER for one line a time. In order to continue the installation process, you must read and agree to this License Agreement, by literally typing the word accept when prompted. Note that typing anything else or nothing at all means you do not agree to the License Agreement and the installation process will stop.

At this point, the installer has acquired all the necessary information and it will begin the install process. Basically, it will install the engines, the binaries and the documentation and it will make the post-install configuration. This is a short list of its actions on your Linux or FreeBSD system:

- Creates the bitdefender user and assigns the installation directory to it.
- Installs the manpages and configures the MANPATH accordingly.
- Appends to the dynamic library loader configuration file the path to the BitDefender libraries.
- Creates a symbolic link to the configuration directory in /etc.
- Integrates BitDefender in the system init scripts.
- Finally, BitDefender Security for Samba is started-up.

5. Uninstall

If you ever need to remove BitDefender Security for Samba, there are several methods to do it, depending on the package type.

First, do not forget to remove the lines you have added to the Samba shares in the `/etc/samba/smb.conf` configuration file. You should remove `bdvfs3` from the `vfs objects` line or even the entire line if no other objects are used. Remove also the configuration lines of bdvfs3 from the same file, if any. They start with something like `bdvfs3:`.

5.1. Uninstall the rpm package

To uninstall BitDefender Security for Samba on an `rpm` package manager based distribution, you have to run the following commands:

```
# rpm -e BitDefender-samba
# rpm -e BitDefender-common
```

5.2. Uninstall the deb package

To uninstall BitDefender Security for Samba using **dpkg**, on a `deb` package manager based distribution, you have to run the following commands:

```
# dpkg -r BitDefender-samba
# dpkg -r BitDefender-common
```

5.3. Uninstall the ipk package

To uninstall BitDefender Security for Samba using **ipkg**, you have to run the following commands:

```
# ipkg-cl remove BitDefender-samba
# ipkg-cl -r BitDefender-common
```

Note
The **ipkg** command must be run from the following location: `/opt/ipkg/bin/`

5.4. Uninstall the tbz package

To uninstall BitDefender Security for Samba you can either use **pkg_delete** command, by running the folowing commands:

```
# pkg_delete bitdefender-samba-{ver}
# pkg_delete bitdefender-common-{ver}
```

Note
Replace {ver} with the version of package returned by the **pkg_info** command.

Or, using **pkg_deinstall**, part of sysutils/portupgrade, run the following command:

```
# pkg_deinstall


 bitdefender-samba
 bitdefender-common
```

Alternative uninstall

You can also uninstall the product this way:

```
# BitDefender-Security-Samba-{ver}-{os}-{arch}.{pkg}\
   .run  --uninstall
```

Getting Started

6. Start-up and Shut-down

BitDefender Security for Samba should be integrated into the system init scripts, in order to start at system initialization and stop at system shut down. Once integrated, the server will be protected all the time, since all BitDefender services will be up and running. Normally, there is no need for the user to manually start or stop BitDefender, but there are administrative tasks when such actions might be necessary. In this chapter you will find how you can safely start and stop the BitDefender services.

The bd8 command

The program **bd(8)**, included in BitDefender programs, plays the role of init script. Among the many parameters it supports, there are the standard `start`, `stop`, `restart`, with obvious actions. The standard location of the program is `/opt/BitDefender/bin/bd`, in case of a standard straight-forward installation. If you have chosen a different installation directory, please use the correct path when calling this program.

As init script, **bd(8)** is symbolically linked, by the install program, to the system specific init directory, such as `/etc/init.d/bd` (for System V type initscripts) or `/etc/rc.d/rc.bd` (for BSD type initscripts). Therefore, according to your distribution, the following commands are identical, doing the same thing in the same way. For example, they will start BitDefender.

```
# /opt/BitDefender/bin/bd start
  - or -
# /etc/init.d/bd start
  - or -
# /etc/rc.d/rc.bd start
  - or -
# service bd start
```

For convenience, the program is always referred to in this document using the first form, but remember you can use all the forms presented above. Use the one that fits you best.

6.1. Start-up

In order to start BitDefender Security for Samba, you have to run the following command (for alternate forms, please see the note above).

```
# /opt/BitDefender/bin/bd start
```

The result will be similar to the screen provided as an example below. Note that if you have more components installed, there will be more corresponding output lines.

```
* Starting bdregd  ...                                  [ ok ]
* Starting bdlogd  ...                                  [ ok ]
* Starting bdscand  ...                                 [ ok ]
* Starting bdfiled  ...                                 [ ok ]
* Starting bdmond  ...                                  [ ok ]
* Starting bdlived  ...                                 [ ok ]
```

Please wait for all the services to be started up. The script will return to the shell when all processes have been initialized. If there are any errors while initializing, they will be reported.

6.2. Shut-down

In order to shut down BitDefender Security for Samba, you have to run the following command (for alternate forms, please see the note above).

```
# /opt/BitDefender/bin/bd stop
```

The output will be similar to the following screen, provided as an example. Note that if you have more components installed and running, there will be more corresponding output lines.

```
* Stopping bdlived  ...                                 [ ok ]
* Stopping bdmond  ...                                  [ ok ]
* Stopping bdscand  ...                                 [ ok ]
* Stopping bdfiled  ...                                 [ ok ]
* Stopping bdlogd  ...                                  [ ok ]
* Stopping bdregd  ...                                  [ ok ]
```

The processes will be shut down in the reverse order of the start up. Please wait for all the services to be stopped. The script will return to the shell when there are no more running processes. If there are any errors while shutting down, they will be reported.

6.3. Restart

A simple restart of all the BitDefender services can be done by running the following command (for alternate forms, please see the note above).

```
# /opt/BitDefender/bin/bd restart
```

The output is similar to those described above.

```
* Stopping bdlived  ...                                    [ ok ]
* Stopping bdmond  ...                                     [ ok ]
* Stopping bdscand  ...                                    [ ok ]
* Stopping bdfiled  ...                                    [ ok ]
* Stopping bdlogd  ...                                     [ ok ]
* Stopping bdregd  ...                                     [ ok ]
* Starting bdregd  ...                                     [ ok ]
* Starting bdlogd  ...                                     [ ok ]
* Starting bdscand  ...                                    [ ok ]
* Starting bdfiled  ...                                    [ ok ]
* Starting bdmond  ...                                     [ ok ]
* Starting bdlived  ...                                    [ ok ]
```

The processes will be shut down in reverse order, then started up. Please wait for all the services to be stopped, then started. The script will return to the shell when the action is complete. If there are any errors while shutting down or starting up, they will be reported.

7. BitDefender Status Output

Since all of its components are daemons, BitDefender works in the background, with little or even no output at all. One source of information about the actions of BitDefender are the logs, if enabled. Instant real-time reports can be obtained by using the built-in facilities of status and statistical reporting.

7.1. Process Status

A short description of all running processes and their process-id (PID) is available on running the following command.

```
# /opt/BitDefender/bin/bd status
```

Invocation of bd8 command
A short discussion about different forms of invoking command **bd(8)** can be found in Chapter 6 "*Start-up and Shut-down*" (p. 21).

Output on non-NPTL systems
On non-NPTL systems, the output is slightly different. Instead on displaying only one thread, all the PIDs of all threads are shown. You should see the multiple process IDs for child threads.

7.2. Basic Information

Using the the text console, more information about the current status of BitDefender is available when issuing the following command:

```
# /opt/BitDefender/bin/bd info
```

Invocation of bd8 command
A short discussion about different forms of invoking command **bd(8)** can be found in Chapter 6 "*Start-up and Shut-down*" (p. 21).

BitDefender Registry
Since this information is stored inside the BitDefender Registry, the **bdregd** daemon should be running in order to see all of it. If not, only a small part will be shown.

The following information is displayed:

- The current version of BitDefender Security for Samba along with some system information.
- The quarantine status.
- The version of installed BitDefender Core Components and Integration Agents.
- The number of signatures, the time when BitDefender last checked for virus signatures updates and the time when it actually updated its signatures.

7.3. Statistical Report

Statistical reports about BitDefender activity can be obtained when running the following command:

```
# /opt/BitDefender/bin/bd stats
```

Invocation of bd8 command
A short discussion about different forms of invoking command **bd(8)** can be found in Chapter 6 "*Start-up and Shut-down*" (p. 21).

8. Fileserver Integration

Due to the internal Samba architecture, the BitDefender VFS can work with only one version of Samba, the one which it was built for. Therefore, the full file name respects the following rule: `bdvfs-{samba_version}.so`, where `{samba_version}` represents the version of Samba the module was built for, such as `3.0.10`. If the package does not contain the VFS module you need for your Samba server, please use the sources from `/opt/BitDefender/var/src` to compile a compatible module.

After the installation you will get an up and running file server virus scanner. To complete the configuration and protect the shares, please refer to the "*Basic Configuration*" (p. 29) section.

If your Samba sources used for compiling VFS module differ from the Samba installed on your Linux distribution, the VFS module should be symlinked into Samba VFS directory. Regarding Samba installation, the location of VFS directory may vary. Depending on your setup, usual locations might be: `/usr/lib/samba/vfs` or `/usr/local/samba/lib/vfs`. The symlink MUST have the name `bdvfs3.so`. To create it, use the following command, replacing the paths and version according to your configuration.

```
# ln -sf /opt/BitDefender/var/lib/samba-vfs/bdvfs-3.0.x.so \\
   /usr/lib/samba/vfs/bdvfs3.so
```

Finally, start smbd daemon (for example run **smbd -D** as root).

8.1. Compiling Samba

If you like to compile Samba, you may follow this example.

- Download the Samba source package, for example `samba-3.0.10.tar.gz`, then run these commands.

```
$ wget http://us4.samba.org/samba/ftp/old-versions/samba-3.0.10.tar.gz
$ tar zxf samba-3.0.10.tar.gz && cd samba-3.0.10/source
$ ./configure --prefix=/usr/local --with-smbmount --with-syslog
$ make headers
$ su -
# make install
```

- Restore your Samba configuration back in `/etc/samba`. You may run **testparm** to check your `smb.conf` file. If **testparm** does not find `smb.conf` file, you must create a symlink in `/usr/local/lib` pointing to the actual `/etc/samba/smb.conf` file.

Advanced Usage

9. Configuration

Once BitDefender Security for Samba has been installed and integrated into the Samba Fileserver, it just works. But there are some settings to fine-tune your installation that you might be interested in.

9.1. Basic Configuration

Here are some hints on fine tuning BitDefender Security for Samba. We will use the **bdsafe** tool for this.

To check the configuration status, run this line:

```
# bdsafe samba status
```

You can see or set the actions to be taken by File Daemon on all malware categories (infected, suspected and riskware), by running this command:

```
# bdsafe samba actions [newactions]
```

The `newactions` parameter must be specified as a list of comma-separated action names. Valid action names are: `disinfect`, `copy-to-quarantine`, `move-to-quarantine`, `delete`, `deny` and `ignore`.

However, you can set the actions to be taken by File Daemon on a particular type of malware, by running one of the following commands:

```
# bdsafe samba oninfected [newactions]
```

```
# bdsafe samba onsuspected [newactions]
```

```
# bdsafe samba onriskware [newactions]
```

Also, you can set the actions to be taken by File Daemon when the first action failed. Run this command:

```
# bdsafe samba failureaction [ignore|deny]
```

9.1.1. Samba VFS Module Configuration

By default, the `smb.conf` file in a pre-defined location (`/etc/samba/smb.conf` for Linux and `/usr/local/etc/smb.conf` for FreeBSD). You can override this default hard-coded search path by running the following command:

```
# bdsafe samba vfs confpath [newpath]
```

The newpath parameter must be the fully-qualified path to the `smb.conf` file, not the directory in which the `smb.conf` file is located (e.g. `/etc/smb.conf` not `/etc`).

Note
The BitDefender Registry Service must be running in order to change the `smb.conf` file location.

To find out detailed information on the status of the BitDefender Samba VFS module, run this command:

```
# bdsafe samba vfs status [sharename]
```

If the optional `sharename` parameter is specified, the information is displayed for that share only.

The BitDefender Samba VFS module is activated/deactivated on a per-share basis. You can activate/deactivate it by running one of the following commands:

```
# bdsafe samba vfs enable [sharename]
```

```
# bdsafe samba vfs disable [sharename]
```

At the same time, you can define a different set of actions to be taken for each share, based on malware type, by running one of the following commands:

```
# bdsafe samba vfs oninfected [sharename] [newacts]
```

```
# bdsafe samba vfs onsuspected [sharename] [newacts]
```

```
# bdsafe samba vfs onriskware [sharename] [newacts]
```

You can set the failure action for the Samba share specified by the `sharename` parameter, by running the following command:

```
# bdsafe samba vfs failureaction [sharename] [newval]
```

9.2. The BitDefender Logger Daemon

The BitDefender Logger Daemon (**bdlogd**) allows you to get a full picture of the others demons activity, as it receives logging messages from the other modules and passes them to the logger plugins.

Either a local socket (Unix domain socket) or a TCP/IP socket will be used to implement communication among different modules of BitDefender while the communication among the Logger Daemon and its plugins is based on API (Application Programming Interface).

bdlogd was designed with a plugins parallel execution philosophy in mind. In short, this means that each plugin will run on its own individual thread. The result is that the slower plugins will no longer disturb the faster ones (like filelog).

To manage the configuration of the Logger Daemon and the associated plugins you will use the **bdsafe** command. You will be provided below with a list of common settings for **bdlogd**.

The general syntax for the **bdlogd** daemon and plugins configuration is the following one:

```
# bdsafe logger configuration [parameters ...]
```

```
# bdsafe logger plugin configuration [parameters ...]
```

The BasePath

To specify the fully-qualified name of a directory from which **bdlogd** will attempt to load plugins, run the following line as root:

```
# bdsafe logger basepath [value]
```

9.2.1. The Logger Plugins

The BitDefender Logger Daemon supports the following plugins:

- The Filelog Plugin
- The SNMP Plugin

The Filelog Plugin

The **bdlogd** receives messages from the other modules and send them to the other plugins, for instance the filelog plugin. By default, the filelog plugin settings are the following:

- bdlived.info=`/opt/BitDefender/var/log/update.log`
- *.error=`/opt/BitDefender/var/log/error.log`
- bdlived.error=`/opt/BitDefender/var/log/update.log`
- *.license=`/opt/BitDefender/var/log/license.log`

It means that, for example, all error-related information, coming from all BitDefender daemons, will be found in this location: `/opt/BitDefender/var/log/error.log`.

However, you can fully customize the daemon and message type and also the file paths where the file logger writes the messages, by using the **bdsafe** command. In order to do this, please run the following line as root:

```
# bdsafe logger file path message_type [value]
```

The `message_type` argument must follow the syntax: `daemon.type`.

`daemon`
: It can take the following values: * (i.e. all daemons), bdmaild, bdfiled, bdlogd, bdscand, bdmond, bdlived

`type`
It can take the following values: * (i.e. all types), info, error, license, debug, virus, spam

You can also enable or disable the entire filelog plugin or just a certain type of message. In order to do this, run these commands as root.

```
# bdsafe logger file disable message_type
```

```
# bdsafe logger file enable message_type
```

Note
For a full description of the filelog settings you must take a look to the bdsafe(8) manual pages.

The SNMP log plugin

By using the **bdsafe** command, you can get the SNMP log plugin status, enable /disable it, set the port number where notification will be sent, set a connection timeout, etc.

For example, to set the port number where notification will be sent, run this command as root.

```
# bdsafe logger snmp port value
```

Note
For a full description of the SNMP log settings you must take a look to the bdsafe(8) manual pages.

9.3. Quarantine

The Quarantine is a special directory (or directories), unavailable for common users, where infected or suspected files or emails are to be isolated for a future purpose. Some BitDefender Daemons (**bdmaild**, **bdfiled** and **bdmond**) add files to Quarantine. The administrator can list and search these files, delete, restore or resend all files that match the given pattern by using the **bdsafe** command.

To find out information about Quarantine directories, run this command as root.

```
# bdsafe quarantine status [quarname]
```

If the optional `quarname` parameter is specified **bdsafe** will display information on that directory only.

To display all files from the `quarname` directory, run this line.

```
# bdsafe quarantine list [quarname]
```

Searching the Quarantine is also very easy. All you have to do is to run this line.

```
# bdsafe quarantine search [quarname] [field] [pattern]
```

The `field` parameter can take one of the following value:

- sender
- recipient
- subject
- uuid

Note
You can use wild-card (*) with the `pattern` parameter (except for the uuid).

To search the specified quarantine directory and copy, move or delete all files that match the specified pattern, run this command.

```
# bdsafe quarantine copy [quarname] [field] [pattern]
```

```
# bdsafe quarantine move [quarname] [field] [pattern]
```

```
# bdsafe quarantine delete [quarname] [field] [pattern]
```

The `field` parameter can take one of the following value:

- sender
- recipient

- subject
- uuid

Note
You can use wild-card (*) with the `pattern` parameter.

To handle the Quarantine configuration, run this command.

```
# bdsafe quarantine configure [quarname] [parameter] [value]
```

`parameter` can take one of the following value:

maxentries
It refers to the maximum number of files allowed in Quarantine.

In this case, the `value` parameter must be a positive integer.

maxsize
It refers to the maximum size of Quarantine allowed.

In this case, the `value` parameter must be a string describing the maximum size of the Quarantine directory. For example, `1m512k` specifies that the maximum size is 1.5 megabytes (`g` is for gigabytes, `m` for megabytes, `k` for kilobytes and `b` for bytes).

ttl
Time-to-live (ttl) refers to a certain time that, when exhausted, would cause the file to be discarded from Quarantine.

In this case, the `value` parameter must be a string describing the maximum amount of time a file can remain in Quarantine before being deleted. For example, `1w2d` specifies that the maximum amount of time a file may remain in the quarantine is one week and two days (`w` is for weeks, `d` for days, `h` for hours, `m` for minutes, `s` for seconds).

10. Product Registration

The product is delivered with a trial registration key valid for thirty days. At the end of the trial period, if you want to continue using the product, you have to provide a new license key.

To check the license status, use the following command.

```
# bdsafe license file
```

You will be presented with the license type, status, the number of covered users and the remaining validity period.

If you have a new license key, the following command will perform the registration of the installed daemon.

```
# bdsafe license file ABCDE12345ABCDE12345
```

11. Testing BitDefender

To make sure BitDefender is really working, you can test its antivirus efficiency using standard testing methods. Basically, you will try to access a special file on a protected fileserver. According to your configuration, you will be allowed or denied access and the file will be disinfected, quarantined, removed or kept in place.

11.1. Antivirus Test

You can verify that the BitDefender Antivirus component works properly by the help of a special test file, known as the *EICAR Standard Anti-virus Test* file. EICAR stands for the *European Institute of Computer Anti-virus Research*. This is a dummy file, detected by antivirus products.

There is no reason to worry, because this file is not a real virus. All that `EICAR.COM` does when executed is display the text `EICAR-STANDARD-ANTIVIRUS-TEST-FILE` and exit.

The reason we do not include the file within the package is that we want to avoid generating any false alarms for those who use BitDefender or any other virus scanner. However, the file can be created using any text editor, provided the file is saved in standard MS-DOS ASCII format and is 68 bytes long. It might also be 70 bytes if the editor puts a CR/LF at the end. The file must contain the following single line:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Copy this line and save the file with any name and `.COM` extension, for example `EICAR.COM`. You can keep the `EICAR.COM` in a safe place and periodically test the server protection.

EICAR online resources

You can visit the EICAR website at http://eicar.com/, read the documentation and download the file from one of the locations on the web page http://eicar.com/anti_virus_test_file.htm.

12. Updates

BitDefender was designed with capabilities for automatic update. At present, the risk of getting infected is high, both because new viruses appear and because the existing ones keep on spreading. This is why your antivirus must be kept up-to-date, by periodically checking the BitDefender servers for new updates.

The BitDefender update process is realized by Live! Update, a daemon which connects periodically to the BitDefender update server and checks whether new virus definitions and product upgrades are available. In case there are any, the daemon will download only the changed files, executing an incremental update and saving bandwidth.

To find out the current configuration settings for the global proxy and the Live! Update service, run the following command.

```
# bdsafe live
```

12.1. Automatic Update

BitDefender Security for Samba is configured to update automatically each hour, through the **bdlived** module. In case of a necessary update, before the specified interval expires, the daemon can be signaled to execute the update routine, manually. To trigger the on-demand check, one can issue the following command.

```
# bdsafe live forceupdate
```

Note
A minimum of five minutes must elapse from the last forced update.

12.1.1. Time Interval Modification

To modify the time interval you will have to run the command bellow. You can change the update interval to the desired value, in seconds. The new value must be an integer between 3600 (seconds, 1 hour) and 86400 (seconds, 24 hours).

```
# bdsafe live checkinterval [new_value]
```

12.1.2. Live! Update Proxy Configuration

If a proxy server is to be used to connect to the Internet, you can set/get your proxy server address and port by using the following command.

```
# bdsafe live globalproxy host [new_host]
```

Whitout the optional `[new_host]` parameter, this command displays the current proxy host only, in case there is a proxy host. To change the host, you must add the `[new_host]` parameter, following this syntax: `host[:port]`

However, you have to enable proxy usage by this command.

```
# bdsafe live globalproxy enabled Y
```

In order to deactivate the use of a proxy, run the following:

```
# bdsafe live globalproxy enabled N
```

For proxy servers that require authentication, the server administrator can set the user domain, name and the associated password via the following commands:

```
# bdsafe live globalproxy user [new_user]
```

```
# bdsafe live globalproxy domain [new_domain]
```

```
# bdsafe live globalproxy password [new_password]
```

The BitDefender Live! Daemon does not immediately load the settings modified via the **bdsafe** command. So, a good idea would be to run the following command, to apply the configuration changes.

```
# bdsafe live reloadsettings
```

12.2. Manual Update

There is one zip archive on the update server, containing the updates of the scanning engines and virus signatures: `cumulative.zip`.

- `cumulative.zip` is released every week on Monday and it includes all the virus definitions and scan engines updates up to the release date.

In order to update the product manually, you should follow these steps.

1. **Download the update file.** Please download `cumulative.zip` and save it somewhere on your disk when prompted.
2. **Extract the updates.** Extract the contents of the zip file to the `/opt/BitDefender/var/lib/scan/Plugins/` directory, overwriting the existing files with the newer ones if necessary.
3. **Files owner and permissions.** After extracting the zip archive, you **must** set the proper owner and permissions, by running the following commands.

```
# chown bitdefender:bitdefender \
 /opt/BitDefender/var/lib/Plugins/*

# chmod 644 /opt/BitDefender/var/lib/Plugins/*
```

4. **Restart BitDefender.** Once updated, BitDefender should be restarted, using the following command.

```
# /opt/BitDefender/bin/bd restart
```

12.3. Patches and New Product Versions

Since the Live! Update module can update automatically only the virus definitions and some of the core libraries used by BitDefender, there is a small tool that can be used to update the whole BitDefender installation.

BitDefender Swiss Army kniFE, **bdsafe(8)**, the multipurpose tool, can be used to keep BitDefender up to date by applying various patches that might appear after the product was released. It can be run directly by the system administrator to list, search, install

or uninstall patches or it can be installed as a cron job to automatically install patches as soon as they are released.

Patches are released to correct any bugs found or to add new features and they are grouped in the following categories: **CRITICAL**, **SECURITY**, **NORMAL**.

- Patches are labeled **CRITICAL** when they affect the normal behavior of the product. For example, if a new kernel is released, preventing the **bdcored** module to accomplish its job, then a **CRITICAL** patch will be released, correcting this issue.
- A patch is labeled **SECURITY** when it has the role of correcting any security related issue. For example, if there is a bug which might permit an attacker to gain access to emails scanned by BitDefender, then a **SECURITY** patch will be released to fix this issue. As opposed to **CRITICAL** patches, which affect BitDefender's normal behavior, **SECURITY** patches can fix the bugs that will not normally occur in a friendly environment, if such one exists.
- Patches labeled **NORMAL** are usually released to fix minor (cosmetic) bugs or to add some new features. For example, if BitDefender incorrectly formats an email header, a **NORMAL** patch will be released to fix this minor issue.

New product versions may bring new features and functionalities. It is recommended to install upgraded versions when they become available.

Administrators are notified about releases of new patches and new product versions via automated e-mails, as well as through the BitDefender Remote Admin interface. Notifications contain all the relevant information regarding the release, such as new features, bug fixes and installation instructions.

Remote Management

13. BitDefender Remote Admin

BitDefender Security for Samba can be configured remotely by using a web browser under any operating system. In order to do this, it is necessary to install on the server side the BitDefender Remote Admin module.

BitDefender Remote Admin is an intuitive management interface. This management tool for UNIX-based product helps you remotely configure any settings in a single interface and lets you check the current status of the product (detailed statistics and update information).

When installing BitDefender Remote Admin, you will be asked to enter a bind address for the Remote Admin server. For security reasons, by default, BitDefender Remote Admin listens for incoming connections on `127.0.0.1 (port 8139)` and allows incoming connections from `127.0.0.1` only, as well. If you want to be able to remotely configure BitDefender, set the address to `0.0.0.0:8139` (listening on all interfaces).

Also as part of the installation you can set a password for the default `administrator` account. If you choose not to, the default password `admin` will be used.

Once the installation is completed, use the `bdcertgen.sh` script located in `/opt/BitDefender/bin/` to indicate your domain name and generate an openssl certificate file. It is highly recommended to enable ssl (secure sockets layer) connections when using remote administration, so make sure you have the Net::SSLeay perl module installed.

To start BitDefender Remote Admin, run the following command:

```
# /opt/BitDefender/bin/bdradmin start
```

After any modification to the configuration, you have to manually restart BitDefender Remote Admin by running the following command:

```
# /opt/BitDefender/bin/bdradmin restart
```

13.1. Getting Started

Once you have setup BitDefender Remote Admin, you can remotely configure almost all BitDefender settings. All you have to do is open your favorite web-browser and

point it to the following location, for the standalone module: http://your.domain.name:8139. The following login form will appear:

Login

To login for the first time, use the default user account.

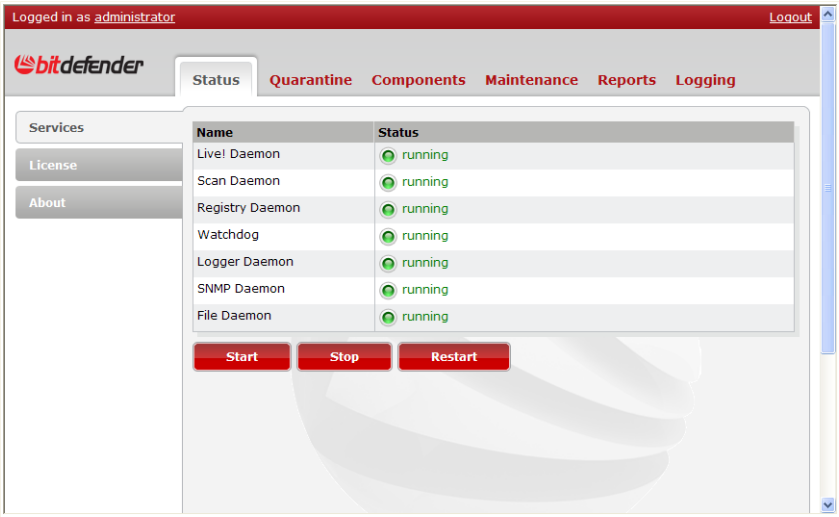
Note
To change the default password, after logging in click **administrator** on the upper left-hand corner of the interface and type the new password in the provided textboxes.

The following sections of this document describe how to configure BitDefender using BitDefender Remote Admin.

13.2. Status

13.2.1. Services

To open this section, go to **Status** and select **Services**.



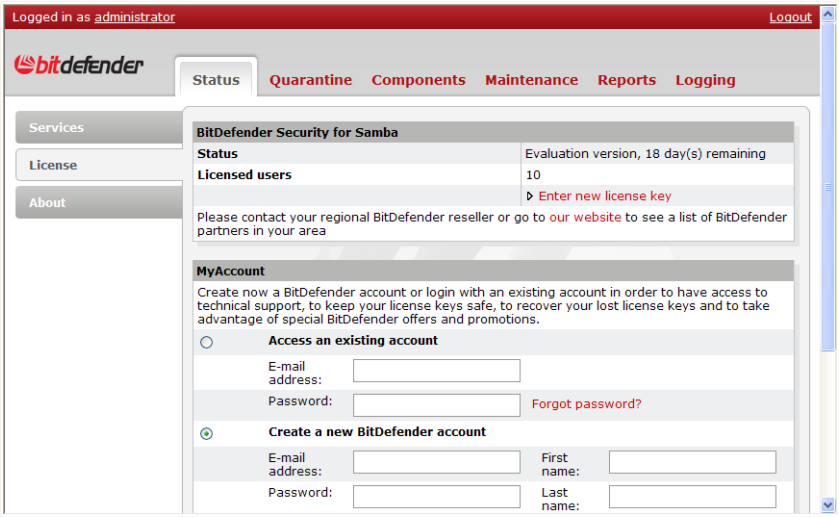
Services

Here you can see a list of all BitDefender services and their current status. You can start, stop or restart the services by clicking the corresponding buttons.

Note
These actions are not performed instantly, a couple of seconds may be required for them to finish.

13.2.2. License

To open this section, go to **Status** and select **License**.



License

Here you can check the license status and register BitDefender.

Click **Enter new license key**, type the license key in the corresponding textbox and click **Apply** to perform the registration process. If you mistype the license key, the message **Invalid key** will be displayed and you will have to type it again.

You can also create a BitDefender account or login to an existing one to have access to technical support, keep your license keys safe, recover your lost license keys and take advantage of special offers and promotions.

To create a BitDefender account, select **Create a new BitDefender account** and provide the required information. The data you provide here will remain confidential.

- **E-mail address** - type in your email address.
- **Password** - type in a password for your BitDefender account.

Note
The password must be at least four characters long.

- **Re-type password** - type in again the previously specified password.

- **First name** - type in your first name.
- **Last name** - type in your last name.
- **Country** - select the country you reside in.

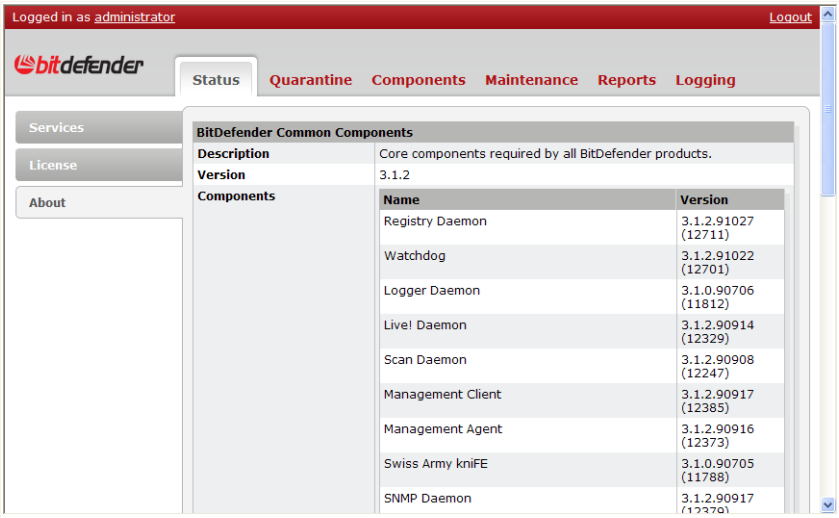
Click **Apply** to finish.

Note
Use the provided email address and password to log in to your account at http://myaccount.bitdefender.com.

To successfully create an account you must first activate your email address. Check your email address and follow the instructions in the email sent to you by the BitDefender registration service.

13.2.3. About

To open this section, go to **Status** and select **About**.



About

This section displays a short description, the version number and the list of components for every BitDefender product installed.

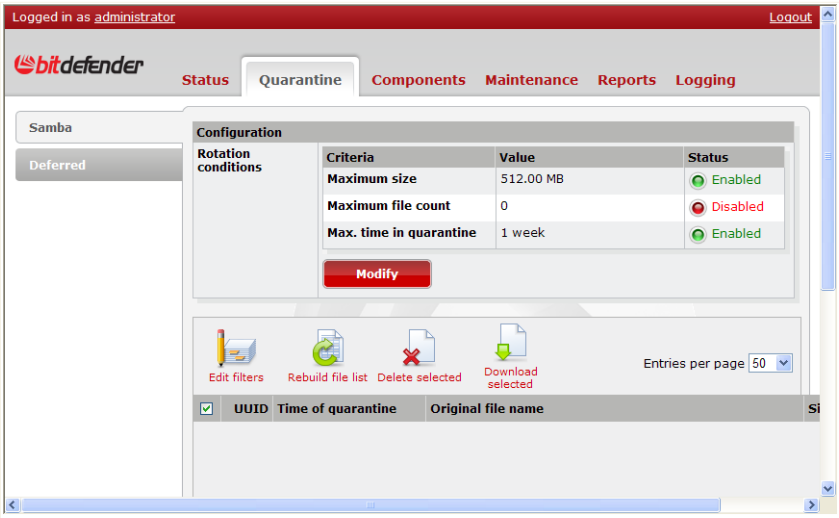
13.3. Quarantine

The Quarantine is a special directory, unavailable for common users, where suspected files are to be isolated for a future purpose.

Quarantined objects are safe
When the virus is in Quarantine it can't do any harm, because it cannot be executed or read.

13.3.1. Samba Quarantine

To open this section, go to **Quarantine** and select **Samba**.



Samba Quarantine

The Samba Quarantine is the directory where infected or suspected files are isolated from the system. The quarantine settings, status and contents are displayed in this window.

You can edit **Samba Quarantine Rotation Conditions** by clicking the **Modify** button and editing the textboxes corresponding to the following criteria:

- **Maximum size** - set a size limit for the quarantine directory. If you type just a number,the limit will be set in bytes. By adding `k`, `m` or `g` after the number you can set the size in Kilobytes, Megabytes or Gigabytes respectively.
- **Maximum file count** - set the maximum number of files the quarantine can contain at one time.
- **Maximum time in quarantine** - set the maximum period of time a file can spend in the quarantine. If you type just a number, the limit will be set in seconds. By adding `m`, `h`, `d` or `w` after the number you can set the time period in minutes, hours, days or weeks respectively.

To disable a condition, type `0` in its corresponding box. Click the **Apply** button to save the changes.

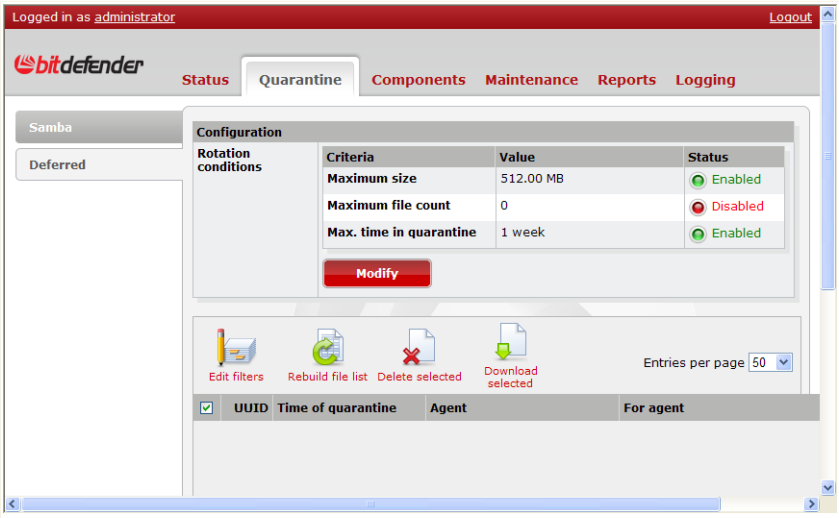
The contents of the quarantine are listed on the lower part of the window. For each item the UUID, time of quarantine, original file name and size are provided. You can use the following tools to easily browse and manage the quarantine:

- **Edit filters** - helps you filter the list of displayed items using the following criteria:
  - **Size** - display items of certain file sizes
  - **Time of quarantine** - display items added to the quarantine within a certain time interval
  - **Original file name** - display items with certain file names
  - **Infection** - filter items based on infection information:
    - **Virus** - display items affected by certain viruses
    - **Status** - display items with certain infection statuses
    - **Performed action** - display items that have been subjected to certain actions by the scanner
    - **Infected object** - display items that are found in certain locations.

  Select the filtering options and click **Apply** to use them on the list.
- **Rebuild the list** - refresh the list of quarantined files.
- **Delete selected** - remove the selected items from the quarantine.
- **Download selected** - select quarantine items and download them to a location of your choice.
- You can choose how many items are to be displayed per page by selecting a number from the **Entries per page** drop-down list.

13.3.2. Deferred Quarantine

To open this section, go to **Quarantine** and select **Deferred**.



Deferred Quarantine

The Deferred Quarantine is an isolated directory storing all the objects that may cause process crashing (for instance, malformed archives or zip-bombs). The quarantine settings, status and contents are displayed in this window.

You can edit **Deferred Quarantine Rotation Conditions** by clicking the **Modify** button and editing the textboxes corresponding to the following criteria:

- **Maximum size** - set a size limit for the quarantine directory. If you type just a number,the limit will be set in bytes. By adding `k`, `m` or `g` after the number you can set the size in Kilobytes, Megabytes or Gigabytes respectively.
- **Maximum file count** - set the maximum number of files the quarantine can contain at one time.
- **Maximum time in quarantine** - set the maximum period of time a file can spend in the quarantine. If you type only a number, the limit will be set in seconds. By adding `m`, `h`, `d` or `w` after the number you can set the time period in minutes, hours, days or weeks respectively.

To disable a condition, type 0 in its corresponding textbox. Click the **Apply** button to save the changes.

The contents of the quarantine are listed on the lower part of the window. For each item the UUID, time of quarantine, agent and for agent are provided. You can use the following tools to easily browse and manage the quarantine:

- **Edit filters** - helps you filter the list of displayed items using the following criteria:
  - **Size** - display items that have certain file sizes
  - **Time of quarantine** - display items added to the quarantine within a certain time interval
  - **Original file name** - display items with certain file names
  - **Agent** - display items quarantined by certain BitDefender modules (i.e. **bdmond**)
  - **For agent** - display quarantine items detected by certain BitDefender modules

  Select the filtering options and click **Apply** to use them on the list.
- **Rebuild the list** - refresh the list of quarantined files.
- **Delete selected** - remove the selected items from the quarantine.
- **Download selected** - download the selected quarantine items to a location of your choice.
- You can choose how many items are to be displayed per page by selecting a number from the **Entries per page** drop-down list.

13.4. Components

To allow sending anonymous reports about the viruses and spam found on your server to the BitDefender Lab, select the **Realtime reporting** checkbox. This way you can help BitDefender identify new viruses and spam and find quick remedies for them.

13.4.1. Samba

To open this section, go to **Components** and select **Samba**.

Components

The Samba file server supports global and per-share Virtual FileSystem Plugins (VFS). The BitDefender VFS module acts as Samba integration agent: aware of the files requested by clients, it can call the BitDefender core to scan the requested files. It receives the scanning results and applies the configured actions, if the file is infected.

If you decide to use the samba integration agent from the BitDefender Remote Admin, there are some options to be configured.

Actions

The order of the actions to be taken when a virus or a suspicious object is found can be specified using the **On Virus**, **On Suspected** and **On Riskware** lists.

The first action to be taken is on top, the last one is at the bottom of the list. Drag and drop the actions up and down the list to indicate the order of the actions to be taken:

- Disinfect
- Delete
- Copy to Quarantine
- Move to Quarantine
- Deny access

- Ignore

Finally, select a **Failure action** from the drop-down list to indicate the action BitDefender will take on objects if the action chosen first has failed: allow or deny access.

Extensions

This is where you can set what kind of files are to be scanned, according to their file extensions. You have three options to choose from, using the corresponding radio button.

All
All files will be scanned, regardless of their file extensions.

Custom
Only the files ended with the file extensions you have typed into the textbox will be scanned. The file extensions must be separated by semicolon (`;`).

Executables
Only the executable files will be scanned.

Apply the changes
To accomplish the setup, do not forget to click the **Apply** button from the corresponding frame for any modification you make.

Maximum File Size

The **Maximum File Size** represents the maximum size (in bytes) of the files that will be considered by the Samba integration agent.

You can type a number into the corresponding textbox, to set a size limit for files scanning.

Virus risk
If a file's size surpasses the limit you have set, the respective file will not be scanned for viruses or other threats.

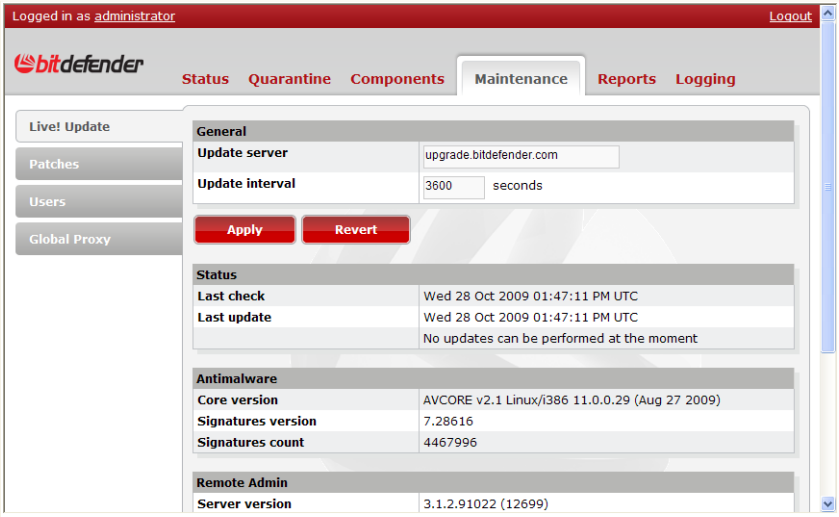
When the value is `0`, no size limit is enforced. All the files, regardless of their size, will be scanned.

Apply the changes
To accomplish the setup, do not forget to click the **Apply** button from the corresponding frame.

13.5. Maintenance

13.5.1. Live! Update

To open this section, go to **Maintenance** and select **Live! Update**.



Live! Update

The Live! Update window provides information regarding the general update settings and update status, the malware signatures version and number of signatures and the BitDefender Remote Admin version.

The default update server is http://upgrade.bitdefender.com and the default update interval is 1 hour. To use a different server or set a different time interval between updates, enter the new information in the corresponding textbox and click **Apply**.

Click the **Update Now!** button to trigger an automatic check and, possibly, update (if there are any updates on the server).

13.5.2. Patches

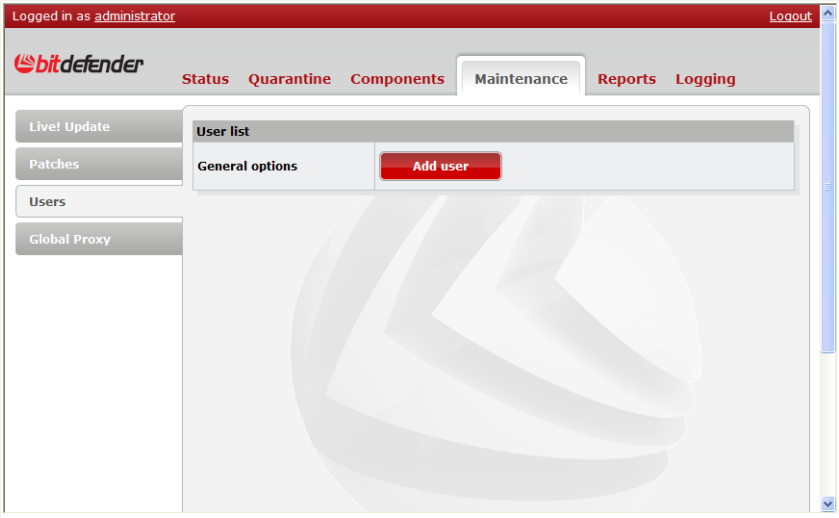
To open this section, go to **Maintenance** and select **Patches**. Patches might appear after the product is released. This is where you are provided with a list of available patches and a short description for each of them.

Choose which patches to install by selecting the checkbox next to them and click the **Update** button to start installing the selected patches.

Important
It is highly recommended to install product patches as soon as they are available.

13.5.3. Users

To open this section, go to **Maintenance** and select **Users**.

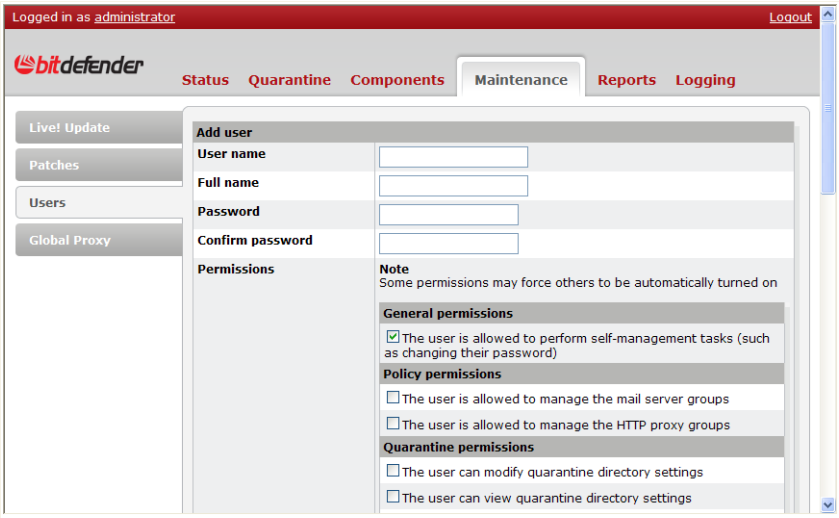


Users

This is where you can create and manage BitDefender Remote Admin user accounts.

Existing users appear in the user list. To view the permissions of a user, click **Show detailed permissions**. To edit the credentials or permissions for a user, click the **Modify** button next to that user. To remove a user, click the **Delete** button.

To create a new user, click **Add user**.

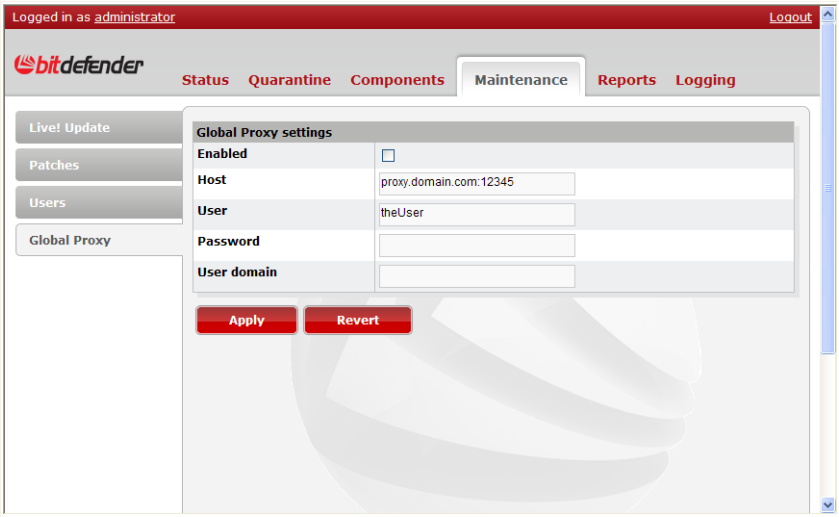


Add New User

Fill in the necessary account information: the user name, the user's full name and account password and set the permissions by selecting their corresponding checkboxes. Click the **Add user** button to finish.

13.5.4. Global Proxy

To open this section, go to **Maintenance** and select **Global Proxy**.



Global Proxy

This is where you can enter the proxy server settings.

If a proxy server is used to connect to the Internet, select the **Enabled** checkbox.

Enter the server address and port in the **Host** textbox. If authentication is required, you also have to enter the user name, password and domain in the corresponding textboxes.

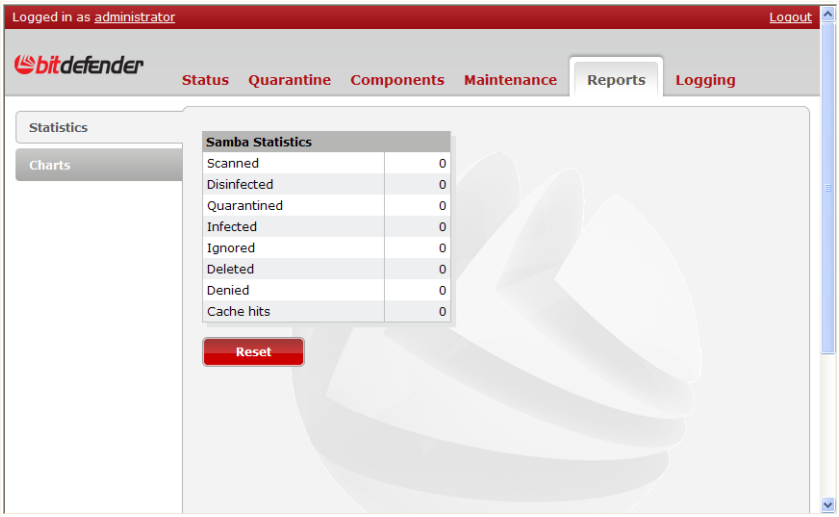
Click **Apply** to save the settings.

13.6. Reports

This section offers the possibility to obtain statistical data regarding product activity as well as showing helpful charts for information related to memory consumption and daemons activity.

13.6.1. Statistics

To open this section, go to **Reports** and select **Statistics**.



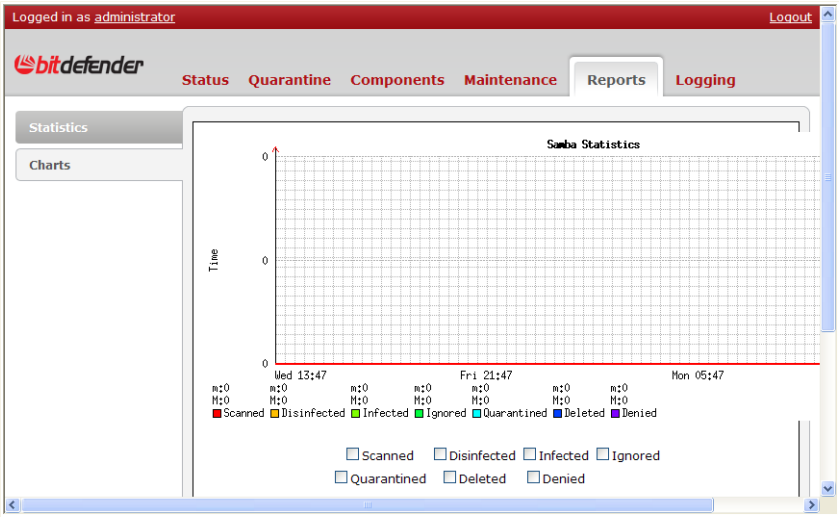
Statistics

The statistical report table can be accessed in this section. Here you can find information regarding the number of scanned objects and the actions taken on them: Scanned, Disinfected, Quarantined, Infected, Ignored, Deleted, Denied, Cache hits.

Use the **Reset** button to clear the statistics.

13.6.2. Charts

To open this section, go to **Reports** and select **Charts**.



Charts

Here you can find two types of charts which you can select from the **Chart type** drop-down list:

- Resource Usage - provides information related to memory consumption and daemons activity
- Samba Statistics - provides information regarding actions taken on scanned objects

You can set which daemons' activity and which actions are to be displayed by selecting the corresponding checkboxes.

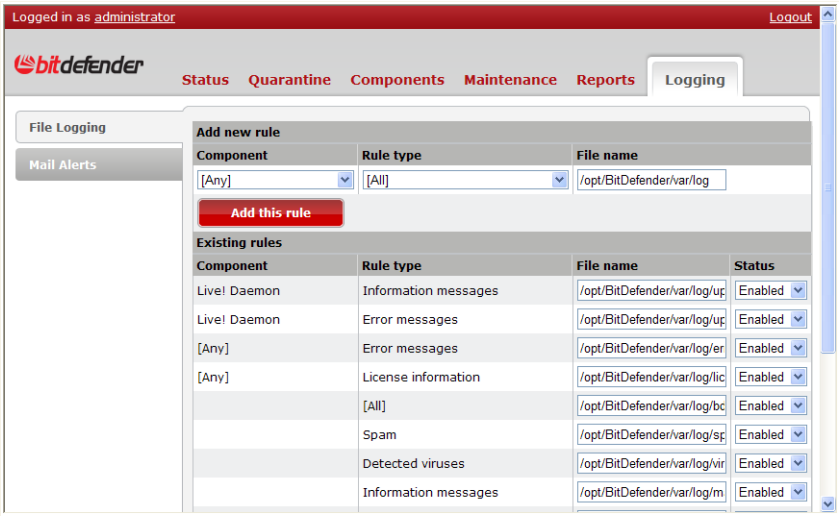
The charts can be customized by selecting different sizes from the **Chart size** drop-down list and different time intervals from the **Interval** drop-down list.

13.7. Logging

This section allows the customization of the logging process, realized by the BitDefender logging module.

13.7.1. File Logging

To open this section, go to **Logging** and select **File Logging**.



File Logging

By default, you will be provided with a list of logging rules. For each rule you can see the component (daemon) it applies to, the rule type, the location of the log file and the status. Enable/disable a rule by selecting the status from the corresponding drop-down list.

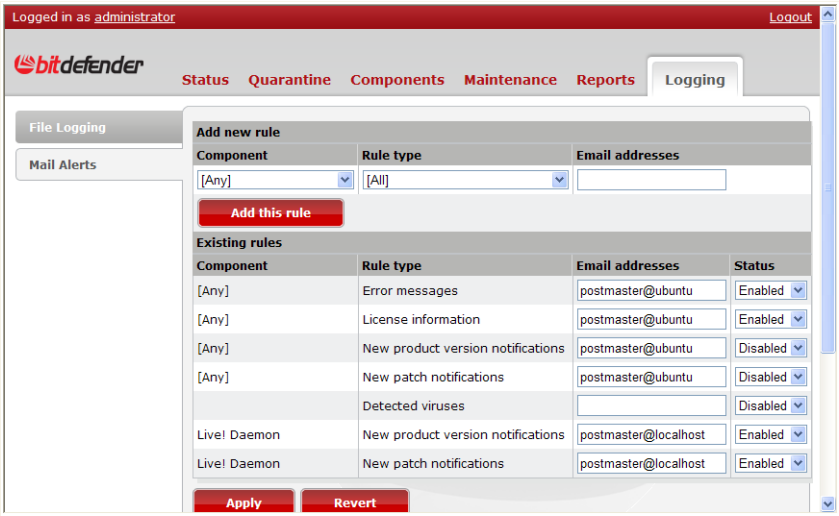
Let's say you enable the **Error messages** for **[Any]** component rule. This means that all error-related information, coming from all BitDefender daemons, will be found in this location: `/opt/BitDefender/var/log/error.log`. Of course, you can easily modify the location by editing the **File name** textbox.

If you want to add a new rule, select the component it applies to and the rule type from the corresponding drop-down lists, type the location of the file into the **File name** textbox and click **Add this rule**.

To complete the setup, click the **Apply** button. To use the default rule set, click the **Revert** button.

13.7.2. Mail Alerts

To open this section, go to **Logging** and select **Mail Alerts**.



Mail Alerts

Mail alerts are simple email messages sent by BitDefender to the system administrator to inform him or her about special events or to the partners of an email communication to inform them about malware found.

By default, you will be provided with a list of logging rules. For each rule you can see the component (daemon) it applies to, the rule type, the email address and the status. Enable/disable a rule by selecting the status from the corresponding drop-down list.

If you want to add a new rule, select the component it applies to and the rule type from the corresponding drop-down lists, type the email address(es) the alerts should be sent to into the **Email addresses** textbox and click **Add this rule**.

To complete the setup, click the **Apply** button. To use the default rule set, click the **Revert** button.

14. SNMP

14.1. Introduction

The SNMP (Simple Network Management Protocol) support of BitDefender consists of two implementations: a SNMP daemon and a Logger plugin.

The SNMP daemon is a custom implementation of a **snmpd** service. It exports a minimal set of features to allow interrogation of BitDefender.

The second implementation, the Logger plugin, is just another module besides the file logger, real-time virus and spam report module or mail notification module. It receives the same BitDefender events information as the others Logger Plugins and it sends them to some remote host running the SNMP trap server, which, in its turn, will process them (send to syslog, etc.).

14.2. The SNMP Daemon

As stated before, this is a daemon which allows the user to interrogate the BitDefender settings.

One popular tool to do SNMP queries is **snmpget**, part of the **net-snmp** package. Each command must follow this syntax:

```
# snmpget -v 1 -Cf -c [community] [hostname] [OID]
```

Let's take an example. Suppose that you want to find out the number of scanned objects on `JohnDoe` server. Simply run this command.

```
# snmpget -v 1 -Cf -c initial JohnDoe \
    1.3.6.1.4.1.22446.1.1.1.1.1.1
```

Below you will find the complete list of the OIDs.

Type	OID
Scanned	1.3.6.1.4.1.22446.1.1.1.1.1.1
Infected	1.3.6.1.4.1.22446.1.1.1.1.1.2

Type	OID
Disinfected	1.3.6.1.4.1.22446.1.1.1.1.1.3
Quarantined	1.3.6.1.4.1.22446.1.1.1.1.1.4
Dropped	1.3.6.1.4.1.22446.1.1.1.1.1.5
LastUpdate	1.3.6.1.4.1.22446.1.1.1.2.1
LastCheck	1.3.6.1.4.1.22446.1.1.1.2.2
CheckSecs	1.3.6.1.4.1.22446.1.1.1.2.3
License/Type	1.3.6.1.4.1.22446.1.1.1.3.1.1
License/Count (user)	1.3.6.1.4.1.22446.1.1.1.3.1.2
License/Count (domain)	1.3.6.1.4.1.22446.1.1.1.3.1.3
bdregd	1.3.6.1.4.1.22446.1.1.3.1.1
bdmond	1.3.6.1.4.1.22446.1.1.3.1.2
bdscand	1.3.6.1.4.1.22446.1.1.3.1.3
bdlogd	1.3.6.1.4.1.22446.1.1.3.1.5
bdlived	1.3.6.1.4.1.22446.1.1.3.1.6
bdmilterd	1.3.6.1.4.1.22446.1.1.3.1.8
bdfiled	1.3.6.1.4.1.22446.1.1.3.1.9

14.3. The BitDefender Logger Plugin

The BitDefender Logger receives messages from various BitDefender components and presents them to the user in various formats. It can log the messages to a file, forward them by email to a designated address or, using this plugin, it can send them to a SNMP server.

14.3.1. Prerequisites

You will need a working SNMP server installed on the same or on some other machine. Please take a look at the Troubleshooting section below, because there are some glitches you have be aware of.

You will also need the following MIB files present in the `mibs` directory we have talked about before: `BITDEFENDER-ALERTS-MIB.txt`, `BITDEFENDER-NOTIFY-MIB.txt` and `BITDEFENDER-TRAP-MIB.txt`.

Regarding the SNMP protocol version, you can use `1`, `2c` or `3` with the following notes.

- Alerts of the `TRAP` type can be sent using the SNMP protocol versions `1` `2c` and `3`.
- Alerts of the `INFORM` type can be sent using the SNMP protocol versions `2c` and `3`.
- Protocol `3` needs the user and offers authentication and encryption.
- Protocols `1` and `2c` need no user, they use the `community` string, which is `public` by default.

14.3.2. Configuration

The messages sent to the SNMP server are received by the **snmptrapd** daemon. We need to configure it. But first, please make sure the SNMP services are not running.

We need a username for the SNMP version 3 protocol. If you want to use version 1 or 2c, you do not need the user and you can skip the following paragraphs.

Let's use the same `bitdefender` username as above. Make sure there is this line in the `/etc/snmp/snmpd.conf` file.

```
rwuser bitdefender
```

Thus we specify that this user who is not yet defined will have read and write access. Add this line at the end of the `/var/net-snmp/snmptrapd.conf` file and remember the passwords should be longer than 8 characters. If the file does not exist, just create it.

```
createUser -e 0xBD224466 bitdefender MD5 <authpass> DES <privpass>
```

If you plan to use the `INFORM` alerts, without need for the EngineID, you will have to add an user without specifying the EngineID. The user defined in the line above will not work, so add a new one.

```
createUser bitdefender_inform MD5 <authpass> DES <privpass>
```

Let's stop a while and explain this line. You are free to change anything in it with the only condition to reflect the changes in the BitDefender configuration.

`-e 0xBD224466`
: This is the EngineID. It is mandatory for alerts of the `TRAP` type and optional for the `INFORM` type. The alert type should be specified in `/BDUX/LoggerDaemon/Plugins/SNMP/AlertType` registry key.

  The EngineID must also be specified in the BitDefender registry at the `/BDUX/LoggerDaemon/Plugins/SNMP/SecurityEngineID` key. If not used (it is optional when the alerts type is `INFORM`), the `SecurityEngineID` key must be empty.

`bitdefender`
: This is the user to create for authenticated SNMP v3. The same name should be declared in the `/etc/snmp/snmpd.conf` (please read above) and in the `/BDUX/LoggerDaemon/Plugins/SNMP/SecurityName` registry key.

`MD5`
: The authentication protocol (`MD5` or `SHA1`) used for authenticated SNMP v3. The same value must be found in `/BDUX/LoggerDaemon/Plugins/SNMP/AuthProto` registry key.

<authpass>
: Set the authentication pass phrase used for authenticated SNMP v3 messages. The same value must be found in the `/BDUX/LoggerDaemon/Plugins/SNMP/AuthProtoPass` registry key.

`DES`
: Set the privacy protocol (`DES` or `AES`) used for encrypted SNMP v3 messages. The same value must be found in the `/BDUX/LoggerDaemon/Plugins/SNMP/SecurityPrivProto` registry key.

<privpass>
: Set the privacy pass phrase used for encrypted SNMP v3 messages. The same value must be found in the `/BDUX/LoggerDaemon/Plugins/SNMP/SecurityPrivProtoPass` registry key.

This line will be replaced with another one, with encrypted passwords, when the **snmptrapd** daemon is started.

One more thing: you do not need to use all the parameters specified above for SNMP v3. You can use the authentication without encryption (the `SecurityLevel` key is

authNoPriv) or no authentication and no encryption (the SecurityLevel key is noAuthNoPriv). You have to modify the createUser line accordingly.

This would be the user. Now, let's get back to the /etc/snmp/snmpd.conf file and add some more lines. You might find them already in your file, but commented out. Uncomment them and set the correct values.

```
# trapsink: A SNMPv1 trap receiver
trapsink  localhost

# trap2sink: A SNMPv2c trap receiver
trap2sink  localhost

# informsink: A SNMPv2c inform (acknowledged trap) receiver
informsink  localhost public

# trapcommunity: Default trap sink community to use
trapcommunity  public

# authtrapenable: Should we send traps when authentication
#                 failures occur
authtrapenable  1
```

I think this is the moment to start the **snmpd** and **snmptrapd** daemons. If you get an error, please review the configuration.

14.3.3. Usage

Now you can test the SNMP server. Here are some commands you may start with. The first one will send the TRAP alert that should be logged on syslog. Please note we use the EngineID.

```
# snmptrap -e 0xBD224466 -v 3 -m ALL -u bitdefender -l authPriv
          -a MD5 -A <authpass> -x DES -X <privpass> localhost 42
          coldStart.0
```

Another command sends an INFORM alert. In this case, there is no need to specify the EngineID and the user you have created must not have the EngineID. In our examples, we have created the bitdefender_inform user for this purpose. The alert will be logged on the syslog too.

```
# snmpinform -v 3 -m ALL -u bitdefender_inform -l authPriv -a MD5
             -A <authpass> -x DES -X <privpass> localhost 42
             coldStart.0
```

If you do not want to use the SNMP version 3 protocol, you can use the other two supported: 1 and 2c. In this case you do not need the username, all you have to know is the community string. This is `public` by default. For example, for version 2c, use this command.

```
# snmptrap -c public -v 2c -m ALL localhost 42 coldStart.0
```

If everything is all right and BitDefender is properly configured (that means the registry keys fit the SNMP server configuration), all you have to do is to enable the plugin (if not already enabled) and try it by sending emails through the MTA. You will shortly see the report on the syslog of the machine running the SNMP server.

14.4. Troubleshooting

Due to some newly found bug in the net-snmp package, the `TRAP` feature does not work for net-snmp version 5.2.2 or newer with the SNMP version 3 protocol (but it works in version 5.2.1). This bug will hopefully be fixed by the net-snmp team soon.

For more information, please see the discussion from the following thread: http://sourceforge.net/mailarchive/forum.php?thread_id=9098786&forum_id=4959.

15. BitDefender Client Security

15.1. Introduction

BitDefender Client Security is a robust and easy-to-use business security and management solution, which delivers superior proactive protection from viruses, spyware, rootkits, spam, phishing and other malware. BitDefender Client Security enhances business productivity and reduces management and malware-related costs by enabling the centralized administration, protection and control of workstations inside companies' networks.

One of the major components of BitDefender Client Security is BitDefender Management Server.

BitDefender Management Server allows centralized management for most BitDefender business solutions installed on network computers, including BitDefender Security for Samba. This type of integration allows you to use the Management Server console to get centralized access to: configuration settings, critical event information and easy-to-interpret statistics.

For more specific information about this type of remote administration of BitDefender Security for Samba, please refer to the BitDefender Management Server Administrator's Guide.

Getting Help

16. Support

16.1. Support department

As a valued provider, BitDefender strives to offer its customers an unparalleled level of fast and accurate support. The Support Center listed below is continually updated with the newest virus descriptions and answers to common questions, so that you obtain the necessary information in a timely manner.

At BitDefender, dedication to saving customers' time and money by providing the most advanced products at the fairest prices has always been a top priority. Moreover, we think that a successful business is based on good communication and a commitment to excellence in customer support.

You are welcome to ask for support at support@bitdefender.com any time. For a prompt response, please include in your email as many details as you can about your BitDefender, about your system and describe the problem as accurately as possible.

16.2. On-line help

16.2.1. BitDefender Knowledge Base

The BitDefender Knowledge Base is an online repository of information about BitDefender products. It stores, in an easily accessible format reports on the results of the ongoing technical support and bug fixing activities of the BitDefender support and development teams, along with more general articles about virus prevention, the management of BitDefender solutions and detailed explanations, and many other articles.

The BitDefender Knowledge Base is open to the public and freely searchable. This wealth of information is yet another way to provide BitDefender customers with the technical knowledge and insight they need. All valid requests for information or bug reports coming from BitDefender clients eventually find their way into the BitDefender Knowledge Base, as bug fix reports, workaround cheatsheets or informational articles to supplement product help files.

The BitDefender Knowledge Base is available any time at http://kb.bitdefender.com.

16.2.2. BitDefender Unix Servers Mailing List

The BitDefender mailing lists bring the latest information regarding security, offer on-line technical support and provide valuable feedback. They are grouped in the following categories.

- Technical Support.
- Product Announcements: bug-fixes, new features or versions, etc.
- Community feedback.

Subscribe and Unsubscribe

In order to join the BitDefender mailing lists, please undertake the following steps:

- Send a blank message to unix-fileservers-subscribe@bitdefender.com with the subject line `subscribe`.
- Confirm your subscription, validate your email address, by redirecting or forwarding the received email from BitDefender to the same address, while leaving the message body unchanged.

To unsubscribe from the mailing list, send an empty mail with the subject `unsubscribe` to unix-fileservers-unsubscribe@bitdefender.com, and follow the received instructions.

Submit a message

To post a message in the list, compose a new message and send it to unix-fileservers@bitdefender.com, with a subject line describing your topic and including all details in your message.

Below are the guidelines and rules of the BitDefender discussion list:

- The official language of BitDefender mailing lists is English.
- Messages must be plain text, instead of HTML or Rich Text.
- All mails should have a short descriptive Subject line, specifying the product you are referring to.
- Necessary details must be included in the messages so that other list members can fully understand the situation.
- The posts may be moderated by the BitDefender Customer Service Department, if the message does not conform to standard and common-sense policies.

16.3. Online Forum

You can also visit our online forum. Please log in to take benefit of the fruitful discussions in the forum.

16.4. Contact information

Efficient communication is the key to a successful business. For the past 10 years BitDefender has established an indisputable reputation in exceeding the expectations of clients and partners, by constantly striving for better a communication. Please do not hesitate to contact us regarding any issues or questions you might have

16.4.1. Web Addresses

Sales department: sales@bitdefender.com
Technical support: http://kb.bitdefender.com
Documentation: documentation@bitdefender.com
Partner Program: partners@bitdefender.com
Marketing: marketing@bitdefender.com
Media Relations: pr@bitdefender.com
Job Opportunities: jobs@bitdefender.com
Virus Submissions: virus_submission@bitdefender.com
Spam Submissions: spam_submission@bitdefender.com
Report Abuse: abuse@bitdefender.com
Product web site: http://www.bitdefender.com
Product ftp archives: ftp://ftp.bitdefender.com/pub
Local distributors: http://www.bitdefender.com/partner_list
BitDefender Knowledge Base: http://kb.bitdefender.com

16.4.2. BitDefender Offices

The BitDefender offices are ready to respond to any inquiries regarding their areas of operation, both in commercial and in general matters. Their respective addresses and contacts are listed below.

North America

BitDefender, LLC
PO Box 667588
Pompano Beach, Fl 33066

Phone (sales&technical support): 1-954-776-6262
Sales: sales@bitdefender.com
Web: http://www.bitdefender.com
Web Self-Service: http://kb.bitdefender.com/site/KnowledgeBase/showMain/2/

Germany

BitDefender GmbH
Airport Office Center
Robert-Bosch-Straße 2
59439 Holzwickede
Deutschland
Phone (office&sales): +49 (0)2301 91 84 222
Phone (technical support): +49 (0)2301 91 84 444
Sales: vertrieb@bitdefender.de
Website: http://www.bitdefender.de
Web Self-Service: http://www.bitdefender.de/site/KnowledgeBase/showMain/2/

UK and Ireland

Business Centre 10 Queen Street
Newcastle, Staffordshire
ST5 1ED
UK
Phone (sales&technical support): +44 (0) 8451-305096
E-mail: info@bitdefender.co.uk
Sales: sales@bitdefender.co.uk
Website: http://www.bitdefender.co.uk
Web Self-Service: http://kb.bitdefender.com/site/KnowledgeBase/showMain/2/

Spain and Latin America

BitDefender España SLU
C/ Balmes, 191, 2º, 1ª
08006 Barcelona
España
Fax: +34 932179128
Phone (office&sales): +34 902190765
Phone (technical support): +34 935026910
Sales: comercial@bitdefender.es
Website: http://www.bitdefender.es

Web Self-Service: http://www.bitdefender.es/site/KnowledgeBase/showMain/2/

Romania

BITDEFENDER SRL
West Gate Park, Building H2, 24 Preciziei Street
Bucharest, Sector 6
Fax: +40 21 2641799
Phone (sales&technical support): +40 21 2063470
Sales: sales@bitdefender.ro
Website: http://www.bitdefender.ro
Web Self-Service: http://www.bitdefender.ro/site/KnowledgeBase/showMain/2/

EMEA and APAC Business Unit

BITDEFENDER SRL
West Gate Park, Building H2, 24 Preciziei Street
Bucharest, Sector 6
Romania
Fax: +40 21 2641799
Phone (sales&technical support): +40 21 2063470
Sales: sales@bitdefender.com
Website: http://www.bitdefender.com
Web Self-Service: http://www.bitdefender.com/site/KnowledgeBase/showMain/2/

Appendices

A. Supported antivirus archives and packs

BitDefender scans inside the most common types of archives and packed files, including, but not limited to the following.

Supported archive types

Ace
Arc
Arj
bzip2
Cab
Cpio (clean+delete)
Gzip (clean+delete)
Ha
Imp
Jar
MS Compress
Lha (lzx)
Rar (including 3.0)
Rpm (clean+delete)
Tar (clean+delete)
Z
Zip (clean+delete)
Zoo

Installation packers

Inno (Inno Installer)
Instyler
VISE (viza.xmd)
InstallShield (ishield.xmd)
Nullsoft Installer (NSIS)
Wise Installer

Mail archives

Dbx (Outlook Express 5, 6 mailboxes)
Mbx (Outlook Express 4 mailbox)
Pst (Outlook mailboxes, supports clean and delete)
Mime (base64, quoted printable, plain) supports clean and delete
Mbox (plain mailbox - Linux and Netscape)
Hqx (HQX is a format used for mail attachments on Mac)
Uudecode
Tnef (a Microsoft format in which some properties of the attachments are encoded, and which can contain scripts)

Supported packers

ACProtect / UltraProtect
PELock NT

ASPack (all versions)
Bat2exec (1.0, 1.2, 1.3, 1.4, 1.5, 2.0)
Yoda's Cryptor
CExe
Diet
DxPack
Dza
Patcher
ECLIPSE
Exe32Pack (1.38)
ExePack
ExeStealth
JdProtect
Lzexe
Mew
Molebox (2.2.3, 2.2.4, 2.2.5, 2.2.6, 2.2.8)
Morphine
Neolite
PC/PE Shrinker 0.71
PCPEC
PE Crypt 32 (1.02 (a,b,c)
PE PACK\CRYPT
PeBundle
pecompact (up to 1.40 beta 3)
PeDiminisher
Pencrypt (3.1, 4.0a, 4.0b)
PePack (all versions)
Perplex
PeShield
PeSpin
Petite (all versions)
Pex
PhrozenCrew PE Shrinker (0.71)
PkLite
PKLITE32 (1.11)
Polyene
RelPack
Rjcrush (1.00, 1.10)
Shrinker (3.3, 3.4)
VgCrypt
Stpe
Telock (all versions)
T-pack
Ucexe
UPolyx
UPX (all versions)
WWPACK32 (1.0b9, 1.03, 1.12, 1.20)
Wwpack (3.01, 3.03, 3.04, 3.04PU, 3.05, 3.05PU)
Xcomor (0.99a, 0.99d, 0.99f (486), 0.99h, 0,99i)

Others

Chm (contains html which can be infected)
Iso (CD images)
Pdf
Rtf
Mso (contains compressed OLE2 files, this way macros are saved in case a Doc is saved as html)
Swf (extracts certain fields that contain various commands; these are scanned by other plug-ins, for ex: SDX)
Bach (extracts debug.exe scripts on the basis of heuristic methods)
Omf (object file)

B. Alert templates

All alerts can be customized. BitDefender provides a template mechanism to generate the alert messages. These templates are plain text files containing the desired notice and certain variables, keywords, which will be replaced with their proper values during the alert generation.

B.1. Variables

The variables and their meaning are described in the table below.

Variable	*Description*
`${BitDefender}`	This variable will be replaced with the *BitDefender* string.
`${Subject}`	The subject of the alert email.
`${Object}`	The object containing the malware.
`${Action}`	The action taken on the object.
`${Virus}`	The virus name.
`${Status}`	The status of the object, namely `Infected`, `Suspected`, `Unknown`.
`${Filename}`	The file found infected.
`${Days}`	The remaining period until key expiration.

The variable ${BitDefender}

It is mandatory to include the variable `${BitDefender}` in your custom template. If it is not found, the module will use the built-in template instead.

These variables can be combined in any form inside the object lists in order to generate a custom template, no matter the language. By default, the templates are stored inside the `/opt/BitDefender/share/templates/`*`language`* directory. For every supported language, there are subdirectory entries, such as `en`, `ro`, `de`, `fr`, `hu`, `es`. Inside the language subdirectories, there are the template files, suggestively named.

Regarding the email alerts, the involved templates are the following: `FileServerAlert.tpl`, `KeyHasExpiredAlert.tpl` and `KeyWillExpireAlert.tpl`.

The template name
You do not have to keep the default file name or location. The only mandatory thing is to refer it accordingly inside the BitDefender Registry, under its corresponding key.

B.2. Sample results

Looking inside the above-mentioned files, one could get confused about their structure. Here are the defaults for the English language and possible results when generating alerts.

B.2.1. FileServer Alert

This is the alert the administrator will receive when an infected file is found on the file server. The variables that could be used are the next ones.

- `${Filename}`
- `${Action}`
- `${Virus}`
- `${Status}`
- `${BitDefender}`

The default template is the following.

```
Subject: System info


${BitDefender} found an infected object in:


File: ${Filename}

Virus: ${Virus}

http://www.bitdefender.com/vfind/?q=${virus}

Status: ${Status}

Action: ${Action}
```

```
Thank you for choosing ${BitDefender}

http://www.bitdefender.com/
```

This will expand to the next message (provided as an example).

```
Subject: System info


BitDefender found an infected object in:


File: eicar.com

Virus: Win32.Klez.A@mm

http://www.bitdefender.com/vfind/?q=Win32.Klez.A@mm

Status: Infected

Action: Deleted


Thank you for choosing BitDefender

http://www.bitdefender.com/
```

B.2.2. KeyWillExpire Alert

This is the alert the system administrator will receive when the license key is about to expire. Variables that could be used:

- `${Days}`
- `${BitDefender}`

The default template is the following.

```
Subject: Registration info


Your ${BitDefender} license will expire in ${Days} days!


http://www.bitdefender.com
```

B.2.3. KeyHasExpired Alert

This is the alert the system administrator will receive when the license key has expired. The variables that could be used are the next ones.

- `${BitDefender}`

The default template is the following.

```
Subject: Registration Error


Your ${BitDefender} license has expired!


http://www.bitdefender.com
```

Glossary

ActiveX

ActiveX is a model for writing programs so that other programs and the operating system can call them. The ActiveX technology is used with Microsoft Internet Explorer to make interactive Web pages that look and behave like computer programs, rather than static pages. With ActiveX, users can ask or answer questions, use push buttons, and interact in other ways with the Web page. ActiveX controls are often written using Visual Basic.

Active X is notable for a complete lack of security controls; computer security experts discourage its use over the Internet.

Archive

A disk, tape, or directory that contains files that have been backed up.

A file that contains one or more files in a compressed format.

Backdoor

A hole in the security of a system deliberately left in place by designers or maintainers. The motivation for such holes is not always sinister; some operating systems, for example, come out of the box with privileged accounts intended for use by field service technicians or the vendor's maintenance programmers.

Boot sector

A sector at the beginning of each disk that identifies the disk's architecture (sector size, cluster size, and so on). For startup disks, the boot sector also contains a program that loads the operating system.

Boot virus

A virus that infects the boot sector of a fixed or floppy disk. An attempt to boot from a diskette infected with a boot sector virus will cause the virus to become active in memory. Every time you boot your system from that point on, you will have the virus active in memory.

Browser

Short for Web browser, a software application used to locate and display Web pages. The two most popular browsers are Netscape Navigator and Microsoft Internet Explorer. Both of these are graphical browsers, which means that they can display graphics as well as text. In addition, most modern browsers can present multimedia information, including sound and video, though they require plug-ins for some formats.

Command line

In a command line interface, the user types commands in the space provided directly on the screen, using command language

Cookie

Within the Internet industry, cookies are described as small files containing information about individual computers that can be analyzed and used by advertisers to track your online interests and tastes. In this realm, cookie technology is still being developed and the intention is to target ads directly to what you've said your interests are. It's a double-edge sword for many people because on one hand, it's efficient and pertinent as you only see ads about what you're interested in. On the other hand, it involves actually "tracking" and "following" where you go and what you click. Understandably so, there is a debate over privacy and many people feel offended by the notion that they are viewed as a "SKU number" (you know, the bar code on the back of packages that gets scanned at the grocery check-out line). While this viewpoint may be extreme, in some cases it is accurate.

Disk drive

It's a machine that reads data from and writes data onto a disk.

A hard disk drive reads and writes hard disks.

A floppy drive accesses floppy disks.

Disk drives can be either internal (housed within a computer) or external (housed in a separate box that connects to the computer).

Download

To copy data (usually an entire file) from a main source to a peripheral device. The term is often used to describe the process of copying a file from an online service to one's own computer. Downloading can also refer to copying a file from a network file server to a computer on the network.

E-mail

Electronic mail. A service that sends messages on computers via local or global networks.

Events

An action or occurrence detected by a program. Events can be user actions, such as clicking a mouse button or pressing a key, or system occurrences, such as running out of memory.

False positive

Occurs when a scanner identifies a file as infected when in fact it is not.

Filename extension

The portion of a filename, following the final point, which indicates the kind of data stored in the file.

Many operating systems use filename extensions, e.g. Unix, VMS, and MS-DOS. They are usually from one to three letters (some sad old OSes support no more than three). Examples include "c" for C source code, "ps" for PostScript, "txt" for arbitrary text.

Heuristic

A rule-based method of identifying new viruses. This scanning method does not rely on specific virus signatures. The advantage of the heuristic scan is that it is not fooled by a new variant of an existing virus. However, it might occasionally report suspicious code in normal programs, generating the so-called "false positive".

Internet Protocol (IP)

A routable protocol in the TCP/IP protocol suite that is responsible for IP addressing, routing, and the fragmentation and reassembly of IP packets.

Java applet

A Java program which is designed to run only on a web page. To use an applet on a web page, you would specify the name of the applet and the size (length and width--in pixels) that the applet can utilize. When the web page is accessed, the browser downloads the applet from a server and runs it on the user's machine (the client). Applets differ from applications in that they are governed by a strict security protocol.

For example, even though applets run on the client, they cannot read or write data onto the client's machine. Additionally, applets are further restricted so that they can only read and write data from the same domain that they are served from.

Macro virus

A type of computer virus that is encoded as a macro embedded in a document. Many applications, such as Microsoft Word and Excel, support powerful macro languages.

These applications allow you to embed a macro in a document, and have the macro execute each time the document is opened.

Mail client

An e-mail client is an application that enables you to send and receive e-mail.

Memory

Internal storage areas in the computer. The term memory identifies data storage that comes in the form of chips, and the word storage is used for memory that exists on tapes or disks. Every computer comes with a certain amount of physical memory, usually referred to as main memory or RAM.

Non-heuristic

This scanning method relies on specific virus signatures. The advantage of the non-heuristic scan is that it is not fooled by what might seem to be a virus, and does not generate false alarms.

Packed programs

A file in a compression format. Many operating systems and applications contain commands that enable you to pack a file so that it takes up less memory. For example, suppose you have a text file containing ten consecutive space characters. Normally, this would require ten bytes of storage.

However, a program that packs files would replace the space characters by a special space-series character followed by the number of spaces being replaced. In this case, the ten spaces would require only two bytes. This is just one packing technique - there are many more.

Path

The exact directions to a file on a computer. These directions are usually described by means of the hierarchical filing system from the top down.

The route between any two points, such as the communications channel between two computers.

Polymorphic virus

A virus that changes its form with each file it infects. Since they have no consistent binary pattern, such viruses are hard to identify.

Port

An interface on a computer to which you can connect a device. Personal computers have various types of ports. Internally, there are several ports for connecting disk drives, display screens, and keyboards. Externally, personal computers have ports for connecting modems, printers, mice, and other peripheral devices.

In TCP/IP and UDP networks, an endpoint to a logical connection. The port number identifies what type of port it is. For example, port 80 is used for HTTP traffic.

Report file

A file that lists actions that have occurred. BitDefender maintains a report file listing the path scanned, the folders, the number of archives and files scanned, how many infected and suspicious files were found.

Script

Another term for macro or batch file, a script is a list of commands that can be executed without user interaction.

Startup items

Any files placed in this folder will open when the computer starts. For example, a startup screen, a sound file to be played when the computer first starts, a reminder calendar, or application programs can be startup items. Normally, an alias of a file is placed in this folder rather than the file itself.

System tray

Introduced with Windows 95, the system tray is located in the Windows taskbar (usually at the bottom next to the clock) and contains miniature icons for easy access to system functions such as fax, printer, modem, volume, and more. Double click or right click an icon to view and access the details and controls.

Transmission Control Protocol/Internet Protocol (TCP/IP)

Transmission Control Protocol/Internet Protocol - A set of networking protocols widely used on the Internet that provides communications across interconnected networks of computers with diverse hardware architectures and various operating systems. TCP/IP includes standards for how computers communicate and conventions for connecting networks and routing traffic.

Trojan

A destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses into your computer.

The term comes from a story in Homer's Iliad, in which the Greeks give a giant wooden horse to their foes, the Trojans, ostensibly as a peace offering. But after the Trojans drag the horse inside their city walls, Greek soldiers sneak out of the horse's hollow belly and open the city gates, allowing their compatriots to pour in and capture Troy.

Update

A new version of a software or hardware product designed to replace an older version of the same product. In addition, the installation routines for updates often

check to make sure that an older version is already installed on your computer; if not, you cannot install the update.

BitDefender has its own update module that allows you to manually check for updates, or let it automatically update the product.

Virus

A program or piece of code that is loaded onto your computer without your knowledge and runs against your will. Most viruses can also replicate themselves. All computer viruses are manmade. A simple virus that can copy itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems.

Virus definition

The binary pattern of a virus, used by the antivirus program to detect and eliminate the virus.

Worm

A program that propagates itself over a network, reproducing itself as it goes. It cannot attach itself to other programs.